25.11.2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

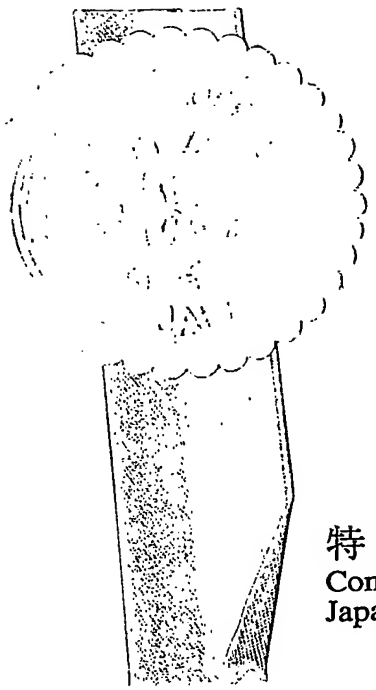
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年１１月２０日

出願番号
Application Number: 特願２００３－３９０２１６

[ST. 10/C]: [ＪＰ２００３－３９０２１６]

出願人
Applicant(s): 日本電気株式会社



２００４年　９月２９日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００４－３０８７１４９

【書類名】　特許願
【整理番号】　33510019
【あて先】　特許庁長官殿
【国際特許分類】　H04M　3/00
　　H04L　9/00
【発明者】
　【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
　【氏名】　須田　幸憲
【発明者】
　【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
　【氏名】　百名　盛久
【特許出願人】
　【識別番号】　000004237
　【氏名又は名称】　日本電気株式会社
【代理人】
　【識別番号】　100093595
　【弁理士】
　【氏名又は名称】　松本　正夫
【手数料の表示】
　【予納台帳番号】　057794
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9303563

【書類名】特許請求の範囲
【請求項１】
無線基地制御局と、前記無線基地制御局に接続される無線基地局とから構成され、前記無線基地局と接続可能な移動端末に対して移動通信サービスを提供する移動通信システムにおいて、
前記無線基地局を私設網内に配置し、前記私設網に設置された中継ノードにより前記私設網上を伝送される前記無線基地制御局と前記無線基地局間の移動通信トラヒックの中継を行い、前記移動端末が発呼あるいは着呼した際に、前記中継ノードが前記私設網内の帯域管理機能と連携した受け付け判定処理を行い、受付が許可された場合に前記移動端末に通信回線を提供することを特徴とする移動通信システム。
【請求項２】
前記移動端末が発呼あるいは着呼した際に、前記無線基地制御局が前記無線基地局宛に送信した帯域制御シグナリングを前記中継ノードが受信することで、前記受付判定処理を起動することを特徴とする請求項１に記載の移動通信システム。
【請求項３】
前記中継ノードが、ＶＰＮゲートウェイであることを特徴とする請求項１又は請求項２に記載の移動通信システム。
【請求項４】
無線基地制御局と、前記無線基地制御局に接続される無線基地局とから構成され、前記無線基地局と接続可能な移動端末に対して移動通信サービスを提供する移動通信システムにおいて、
前記無線基地局を私設網内に配置し、前記私設網に設置された中継ノードにより前記私設網上を伝送される前記無線基地制御局と前記無線基地局間の移動通信トラヒックの中継を行い、
前記無線基地制御局と前記中継ノード間では第１の暗号鍵を、前記無線基地局と中継ノード間では第２の暗号鍵を用いて暗号化通信を行い、
前記第２の暗号鍵の生成に必要な秘匿鍵を前記無線基地制御局と前記無線基地局間の鍵交換メカニズムにより生成し、前記無線基地制御局が前記中継ノードに前記秘匿鍵を通知することを特徴とする移動通信システム。
【請求項５】
無線基地制御局と、前記無線基地制御局に接続される無線基地局とから構成され、前記無線基地局と接続可能な移動端末に対して移動通信サービスを提供する移動通信システムにおいて、
前記無線基地局を私設網内に配置し、前記無線基地局と前記私設網を介して接続される中継ノードと前記無線基地局間の前記移動通信トラヒックは前記私設網内を伝送され、前記中継ノードにより前記私設網上を伝送される前記無線基地制御局と前記無線基地局間の移動通信トラヒックの中継を行い、
前記無線基地制御局と前記中継ノード間では第１の暗号鍵を、前記無線基地局と中継ノード間では第２の暗号鍵を用いて暗号化通信を行い、
前記第２の暗号鍵を前記無線基地制御局と前記無線基地局間の鍵交換メカニズムにより動的に生成し、前記無線基地制御局が前記中継ノードに前記第２の暗号鍵を通知することを特徴とする移動通信システム。
【請求項６】
前記無線基地制御局が、
前記暗号鍵の生成に必要となる事前共有鍵を前記無線基地局との間で鍵交換メカニズムを用いて動的に生成する手段と、前記事前共有鍵を前記中継ノードに通知する手段とを備えることを特徴とする請求項４又は請求項５に記載の移動通信システム。
【請求項７】
前記無線基地制御局が、
前記無線基地局との間で鍵交換メカニズムを用いて動的に前記暗号鍵を生成する手段と

、前記暗号鍵を前記中継ノードに通知する手段とを備えることを特徴とする請求項４又は請求項５に記載の移動通信システム。

【請求項８】

無線基地局と無線基地制御局間の移動通信トラヒックの中継を行う中継ノードにおいて、

前記無線基地局が設置される私設網に設置され、前記私設網上を伝送される前記無線基地制御局と前記無線基地局間の移動通信トラヒックの中継を行い、

前記無線基地制御局が前記無線基地局宛に送信した帯域制御シグナリングを受信する手段と、

該帯域制御シグナリングに含まれるトラヒック情報を抽出する手段と、

私設網内の帯域管理機構と連携して受け付け判定を行う手段と、

前記受付判定結果と前記受付許可された帯域制御情報を含む帯域制御シグナリングを送信する手段を備えることを特徴とする中継ノード。

【請求項９】

無線基地局と無線基地制御局間の移動通信トラヒックの中継を行う中継ノードにおいて、

前記無線基地局が設置される私設網に設置され、前記私設網上を伝送される前記無線基地制御局と前記無線基地局間の移動通信トラヒックの中継を行い、

無線基地局と無線基地制御局に接続され、前記無線基地局とは第１の暗号鍵を、前記無線基地制御局とは第２の暗号鍵を用いて暗号化通信を行い、

前記無線基地制御局から前記第１の暗号鍵を生成するための事前共有鍵を受け取る手段と、前記事前共有鍵を用いて前記無線基地局との間で前記第１の暗号鍵を動的に生成する手段と、前記第１の暗号鍵を用いて前記移動通信トラヒックの暗号化を行う手段とを備えることを特徴とする中継ノード。

【請求項１０】

無線基地局と無線基地制御局間の移動通信トラヒックの中継を行う中継ノードにおいて、

前記無線基地局が設置される私設網に設置され、前記私設網上を伝送される前記無線基地制御局と前記無線基地局間の移動通信トラヒックの中継を行い、

無線基地局と無線基地制御局に接続され、前記無線基地局とは第１の暗号鍵を、前記無線基地制御局とは第２の暗号鍵を用いて暗号化通信を行い、

前記第１の暗号鍵を前記無線基地制御局から受け取る手段と、前記第１の暗号鍵を用いて前記移動通信トラヒックの暗号化を行う手段とを備えることを特徴とする中継ノード。

【請求項１１】

複数の無線基地局と異なる暗号鍵を用いて暗号化通信を行う中継ノードを介して、前記無線基地局と接続される無線基地制御局において、

前記暗号鍵の生成に必要となる事前共有鍵を前記無線基地局との間で鍵交換メカニズムを用いて動的に生成する手段と、前記事前共有鍵を前記中継ノードに通知する手段とを備えることを特徴とする無線基地制御局。

【請求項１２】

複数の無線基地局と異なる暗号鍵を用いて暗号化通信を行う中継ノードを介して、前記無線基地局と接続される無線基地制御局において、

前記無線基地局との間で鍵交換メカニズムを用いて動的に前記暗号鍵を生成する手段と、前記暗号鍵を前記中継ノードに通知する手段とを備えることを特徴とする無線基地制御局。

【請求項１３】

無線基地局と無線基地制御局間の移動通信トラヒックの中継を行う中継ノードで実行される中継ノード用プログラムであって、

無線基地局が設置される私設網に設置され、前記私設網上を伝送される無線基地制御局と前記無線基地局間の移動通信トラヒックの中継を行う機能と共に、

前記無線基地制御局が前記無線基地局宛に送信した帯域制御シグナリングを受信する機能と、前記帯域制御シグナリングに含まれるトラヒック情報を抽出する機能と、私設網内の帯域管理機構と連携して受け付け判定を行う機能と、前記受付判定結果と前記受付許可された帯域制御情報を含む帯域制御シグナリングを送信する機能とを有することを特徴とする中継ノード用プログラム。

【請求項１４】

無線基地局と無線基地制御局間の移動通信トラヒックの中継を行う中継ノードで実行される中継ノード用プログラムであって、

無線基地局が設置される私設網に設置され、前記私設網上を伝送される無線基地制御局と前記無線基地局間の移動通信トラヒックの中継を行い、前記無線基地局とは第１の暗号鍵を、前記無線基地制御局とは第２の暗号鍵を用いて暗号化通信を行う機能と共に、

前記無線基地制御局から前記第１の暗号鍵を生成するための事前共有鍵を受け取る機能と、前記事前共有鍵を用いて前記無線基地局との間で前記第１の暗号鍵を動的に生成する機能と、前記第１の暗号鍵を用いて前記移動通信トラヒックの暗号化を行う機能とを有することを特徴とする中継ノード用プログラム。

【請求項１５】

無線基地局と無線基地制御局間の移動通信トラヒックの中継を行う中継ノードで実行される中継ノード用プログラムであって、

無線基地局が設置される私設網に設置され、前記私設網上を伝送される無線基地制御局と前記無線基地局間の移動通信トラヒックの中継を行い、前記無線基地局とは第１の暗号鍵を、前記無線基地制御局とは第２の暗号鍵を用いて暗号化通信を行う機能と共に、

前記第１の暗号鍵を前記無線基地制御局から受け取る機能と、前記第１の暗号鍵を用いて前記移動通信トラヒックを暗号化する機能とを有することを特徴とする中継ノード用プログラム。

【請求項１６】

複数の無線基地局と異なる暗号鍵を用いて暗号化通信を行う中継ノードを介して、前記複数の無線基地局と接続される無線基地制御局で実行されるプログラムであって、

前記暗号鍵の生成するために必要な事前共有鍵を前記無線基地局との間で鍵交換メカニズムを用いて動的に生成する機能と、前記事前共有鍵を前記中継ノードに通知する機能とを有することを特徴とする無線基地制御局用プログラム。

【請求項１７】

複数の無線基地局と異なる暗号鍵を用いて暗号化通信を行う中継ノードを介して、前記複数の無線基地局と接続される無線基地制御局に使用されるプログラムであって、

前記無線基地局との間で鍵交換メカニズムを用いて動的に前記暗号鍵を生成する機能と、前記暗号鍵を前記中継ノードに通知する機能とを有することを特徴とする無線基地制御局用プログラム。

【書類名】明細書
【発明の名称】移動通信システム、中継ノード、無線基地制御局、中継ノード用プログラム、無線基地制御局用プログラム
【技術分野】
【０００１】
本発明は、複数の無線基地制御局と、１つの無線基地制御局に接続される複数の無線基地局とから構成され、無線基地局と接続可能な移動端末に対して移動通信サービスを提供する移動通信システムに関し、特に、私設網を利用して屋内エリア内のユーザに対して移動通信サービスを提供することを可能にする移動通信システムに関する。
【背景技術】
【０００２】
移動通信システムでは、ビル等の屋内の内部まで電波が届きにくいため、屋内で移動端末を使用するユーザは安定した移動通信サービスを受けることができない。屋内のユーザに対して安定した移動通信サービスを提供するためには、屋内をカバーするための移動通信専用の屋内システムの導入が必要となる。特に、２ＧＨｚ帯を使用する３Ｇサービスは２Ｇサービスと比べて、電波伝搬特性が良くないため、不感地帯となる屋内エリアが多くなる。
【０００３】
このような状況において、３Ｇサービスの屋内エリアを２Ｇサービスと同等にするためには、屋内システムを多数導入することが必要となるが、それに応じて移動通信オペレータを多数配置することはコスト的な点で実現が難しい。そのため、より低コストな屋内システムが要求されている。
【０００４】
ＵＭＴＳの標準化を行っている３ＧＰＰでは、無線基地制御局（ＲＮＣ）と無線基地局間をＩＰ網で接続可能とするＩＰトランスポートオプションを提供するリリース５が定義された。そこで、ＩＰトランスポートを利用した屋内システムの１つのアプローチとして、屋外回線に公衆インターネット網や閉域ＩＰ網、屋内回線にＬＡＮ等の私設網（例えば、企業等が自身で私的に構築したネットワーク等）を利用する形態が考えられる。これにより、回線敷設コストを大幅に削減でき、屋内システムの導入コストを大幅に低減可能となる。
【０００５】
このような私設網（ネットワーク）を用いた移動通信システムでは、以下に示す新たな機能が要求される。
（１）私設網における移動通信トラヒックの帯域制御
（２）私設網内のファイアウォール／ＮＡＰＴ(Network Address Port Translation)を越えた無線基地制御局－無線基地局間通信の実現
（３）移動通信トラヒックのセキュリティ確保
（４）移動通信オペレータが移動通信ノードに対して独自に割り当てたＩＰアドレス体系の維持
【０００６】
上記（１）の機能に関して、私設網での帯域制御方法として、ポリシーサーバによる集中型帯域制御方式が一般的である。本方式は、ポリシーサーバがルータやイーサネット(R)スイッチ等のＬＡＮデバイスに対してパケット識別に必要となるトラヒック情報と帯域制御ルールを含む帯域制御情報を事前に配布し、私設網のエッジに位置するＬＡＮデバイスがトラヒック情報に基づきエンドホストあるいはインターネットから受信したパケットのＩＰヘッダとＬ４ヘッダを用いてパケット識別を行い、該当する帯域制御情報に応じたマークをパケットに付加した後、次ホップのＬＡＮデバイスに転送する。エッジでないＬＡＮデバイスは、エッジのＬＡＮデバイスが付加したマークとポリシーサーバから配布された帯域制御情報に基づきパケット単位で帯域制御を行うものである。
【０００７】

上記（２）～（４）の機能に関しては、例えばＩＰｓｅｃベースのＶＰＮ(Virtual Private Network：仮想私設ネットワーク)技術を利用することで実現可能である。具体的には、ＶＰＮゲートウェイを私設網の管轄外に設置し、無線基地制御局と無線基地局は常にＶＰＮゲートウェイを介して通信を行い、無線基地制御局とＶＰＮゲートウェイ間、無線基地制御局と無線基地局間においてＩＰｓｅｃによる暗号化通信技術を適用することで実現できる。

【０００８】

なお、従来の移動通信システムの例としては、例えば、セキュリティを維持しつつ、無線端末装置と有線端末装置間で通信を行うための技術が、特開２００１－３３３１１０号公報（特許文献１）等に開示されている。

【０００９】

従来の移動データ通信における仮想私設網の構成方法に関する技術が、例えば特開平１０－０３２６１０号公報（特許文献２）に開示されている。

【特許文献１】特開２００１－３３３１１０号公報

【特許文献２】特開平１０－０３２６１０号公報

【発明の開示】

【発明が解決しようとする課題】

【００１０】

上記の帯域制御方式において、移動通信トラヒックが私設網の帯域の大半を占有した場合、私設網の回線が輻輳し、無線基地制御局－無線基地局間の移動通信トラヒックの通信品質が劣化する、あるいは他の私設網内のトラヒックに支障をきたす可能性がある。

【００１１】

また、上記のＶＰＮ方式では、無線基地制御局及び無線基地局が複数存在する場合、無線基地制御局と無線基地局間の経路制御情報をＶＰＮゲートウェイに、第三者認証を利用せずに無線基地制御局－ＶＰＮゲートウェイ間とＶＰＮゲートウェイ－無線基地局間でのＩＰｓｅｃ　ＳＡ(Security Association)を確立する上で必要となる事前共有鍵をＶＰＮゲートウェイに予め設定しておく必要があり、設置する無線基地局の台数が多くなった場合に、屋内システムの導入時の作業が煩雑になる。

【００１２】

本発明の目的は、私設網を用いて移動通信サービスを提供するに当たり、移動通信トラヒックの増大に起因して私設網内回線が輻輳するのを防ぎ、他のトラヒックにも支障をきたさない移動通信システムを提供することにある。

【００１３】

本発明の他の目的は、設置する無線基地局の台数が多くなった場合にも、屋内システムの導入時の作業を簡易化することができる移動通信システムを提供することにある。

【課題を解決するための手段】

【００１４】

本発明によれば、移動端末が発呼/着呼した際に、無線基地制御局と無線基地局間の移動通信制御シグナリングを中継ノードであるＶＰＮゲートウェイが終端し、シグナリングに含まれるトラヒック情報をポリシーサーバに通知すると共に、受付判定を要求する。ポリシーサーバが受付を許可した場合のみ、移動端末に通信回線を提供することにより、上記の目的を達成する。

【００１５】

本発明の他の態様によれば、中継ノードであるＶＰＮゲートウェイと無線基地制御局間に既にＳＡが確立されている状態で、無線基地局を起動すると、ＶＰＮゲートウェイに対して転送先無線基地制御局を指定した後、ＳＡ確立処理を開始し、ＶＰＮゲートウェイは、ＳＡを確立するためのＩＫＥ(Internet Key Exchange)シグナリングを、指定された転送先無線基地制御局に転送し、無線基地制御局が代理でＳＡを確立し、ＶＰＮゲートウェイに対して確立したＳＡ情報を通知する。

【００１６】

あるいは、無線基地局と無線基地制御局間でSAの確立に必要となる事前共有鍵を動的に生成し、無線基地制御局がＶＰＮゲートウェイに事前共有鍵を通知し、ＶＰＮゲートウェイはこれを用いて無線基地局との間でSAを動的に確立する。このように、ＶＰＮゲートウェイは無線基地制御局より通知されたSA情報、あるいは配布された事前共有鍵を用いて確立したSA情報に基づき、無線基地局との間で暗号化通信を行うことにより、上記の目的を達成する。

【発明の効果】

【００１７】

本発明の第１の効果は、無線基地局と無線基地制御局間の回線として私設網を用いて移動通信サービスを提供するに当たり、移動通信トラヒックに起因して私設網内の回線が輻輳するのを防ぎ、他のトラヒックに支障をきたさないことである。これは、移動端末が発呼／着呼した際に、無線基地制御局が送信する移動通信制御シグナリングを中継ノードであるＶＰＮゲートウェイが受信し、移動端末の通信に必要となる帯域をポリシーサーバに通知すると共に、受付判定を要求し、受付判定の結果に応じて移動端末の通信回線を提供するか否かを決定するためである。

【００１８】

本発明の第２の効果は、屋内システムの導入時の作業を簡易化できることである。これは、無線基地局が起動すると、中継ノードであるＶＰＮゲートウェイに対してＩＫＥシグナリングを転送する依頼した後、無線基地局とＶＰＮゲートウェイ間で利用するＳＡを無線基地局と無線基地制御局間で確立し、無線基地制御局が確立したＳＡ情報をＶＰＮゲートウェイに通知すると共に、ＶＰＮゲートウェイは通知されたＳＡ情報を利用して無線基地局と暗号化通信を行うようにしたためである。あるいは、ＩＰｓｅｃ　ＳＡ確立に必要な事前共有鍵を無線基地局と無線基地制御局間で鍵交換メカニズムにより動的に生成し、無線基地制御局が生成した事前共有鍵をＶＰＮゲートウェイに通知し、ＶＰＮゲートウェイは配布された事前共有鍵を用いて無線基地局との間にＩＰｓｅｃ　ＳＡを確立し、暗号化通信を行うためである。

【実施例】

【００１９】

図１及び２に示すネットワーク構成図を用いて本発明の第１の実施例に係わる移動通信システムを説明する。ＰＣ１１０等が接続された私設の網であるＬＡＮ２０は、イーサネット(R) (Ethernet(R)) で構築されており、ファイアウォール９０、VPN(Virtual Private Netowork)ゲートウェイ(GateWay)１００を介してインターネット網１０と接続されている。一方、移動通信コア網３０は無線基地制御局（無線基地制御局:Radio Network Controllerと称する）７０と移動網ゲートウェイ１２０を介してインターネット網１０と接続されている。

【００２０】

また、無線基地局６０～６３は私設網（私設ネットワーク、例えば企業が私的に構築したネットワーク）としてのＬＡＮ２０に接続され、無線基地制御局７０と無線基地局６０～６３間の通信では、インターネット網１０及びＬＡＮ２０を回線として利用し、ＶＰＮゲートウェイ１００を介することでファイアウォール９０を越えた通信を行う。このような形態で、移動通信オペレータは移動端末８０に対してインターネットアクセス等のデータ通信サービスを提供する。

【００２１】

さらに、ＬＡＮ２０内はプライベートアドレスで運用されており、インターネット網１０はグローバルアドレスで運用されている。無線基地制御局７０と無線基地局６０～６３間の通信では、セキュリティを確保するためＩＰｓｅｃ　ＥＳＰ(Encapsulation Security Payload)トンネルモードを利用し、インターネット網１０では外部ＩＰヘッダにグローバルＩＰアドレスを、ＬＡＮ２０ではプライベートＩＰアドレスを使用し、内部ＩＰヘッダにはオペレータが無線基地制御局７０及び無線基地局６０～６３に独自に割り当てたＩＰアドレス（以降、オペレータ独自アドレスと称する）を使用する。

【００２２】
ＬＡＮ２０は例えば図２のように構成される。図示するように、ＬＡＮ２０はルータ２１０と複数のＥｔｈｅｒｎｅｔ(R)スイッチ２２０～２２３で構成されており、無線基地局６０とＰＣ１１０はそれぞれＥｔｈｅｒｎｅｔ(R)スイッチ２２１、２２３に接続されている。（記述を簡略化するため、以降ではルータ２１０とＥｔｈｅｒｎｅｔ(R)スイッチ２２０～２２３を総称してＬＡＮデバイスと呼ぶ。）また、ＬＡＮ２０では帯域制御が行われており、本実施例ではポリシーサーバ２００による集中型の帯域制御を行っている場合を示している。その場合、ポリシーサーバ２００にはトラヒックの特性が記述されたトラヒック情報とそのトラヒックに対して帯域制御を行う上で必要となる帯域制御情報が予め設定されており、ポリシーサーバ２００はＬＡＮデバイスの起動を検出すると、ＣＯＰＳ(Common Open Policy Service)プロトコルを用いてトラヒック情報と帯域制御情報をＬＡＮデバイスに配信し、各ＬＡＮデバイスは通知された帯域制御情報に基づいて受信したパケットに対して帯域制御を行う。
【００２３】
また、各ＬＡＮデバイスは帯域の制御状態をＳＮＭＰ(Simple Network Management Protocol)によりポリシーサーバ２００にレポートし、ポリシーサーバ２００はＬＡＮ２０全体の帯域制御状態を集中的に管理する。ＬＡＮ２０を流れる移動通信トラヒックに対しても同様の帯域制御が行われる。移動通信トラヒックにはシグナリングデータとユーザデータの２種類がある。シグナリングデータトラヒックに関しては以下に述べる手法により帯域制御を行う。予めポリシーサーバ２００にシグナリングデータのトラヒック情報と帯域制御情報を設定しておき、ポリシーサーバが各ＬＡＮデバイスに配信することで、各ＬＡＮデバイスはシグナリングデータトラヒックに対して帯域制御を行う。また、ユーザデータに関しては以下に述べる手法により帯域制御を行う。
【００２４】
移動端末８０が発呼あるいは着呼した際に無線基地制御局７０が送信するＱｏＳシグナリングをＶＰＮゲートウェイ１００が受信し、ＶＰＮゲートウェイ１００がＱｏＳシグナリングに含まれるユーザデータのトラヒック情報を抽出し、トラヒック情報をポリシーサーバ２００に通知する。ポリシーサーバ２００がトラヒック情報に記載の帯域を許容できるか否かの受付判定を行う。ポリシーサーバ２００が受付を許可した場合は、受付を許可した帯域制御情報及びトラヒック情報を移動通信トラヒックの経路上のＬＡＮデバイス、あるいはすべてのＬＡＮデバイスに配信し、移動通信トラヒックの経路上のＬＡＮデバイスはユーザデータトラヒックに対して通知された情報に基づき帯域制御を行う。
【００２５】
次に、図３～図６を参照して、本発明の第１の実施例に係る移動通信システムを構成する無線基地制御局７０、無線基地局６０、６１、６２、６３、ＶＰＮゲートウェイ１００及びポリシーサーバ２００の構成を説明する。
【００２６】
無線基地制御局７０は、例えば図３に示すような構成を備えている。具体的に説明すると、無線基地制御局７０は、移動通信コア網側ＩＦ３００とインターネット側ＩＦ３１０の２つのインタフェースを備え、Ｌ２処理部３２０、４１０、ＩＰトランスポート処理部４３０、移動無線通信プロトコル処理部３３０、移動無線通信制御部３６０、帯域制御処理部４４０を備えて構成される。
【００２７】
このうち、移動無線通信プロトコル処理部３３０の内部には、シグナリング処理部３４０とユーザデータ処理部３５０がある。ＩＰトランスポート処理部４４０の内部には、ＩＰ処理部３８０、Ｌ４処理部３７０、ＩＰｓｅｃ処理部４１０がある。ＩＰｓｅｃ処理部４１０はＥＳＰ(Encryption Security Payload)　ＳＡ(Security Association)情報４２０を保持する。これらの各処理部における基本的な処理を以下で説明する。
【００２８】
移動通信コア網側ＩＦ３００から受信したシグナリングデータ及びユーザデータは、Ｌ

２処理部４１０でリンク処理が行われた後、インターネット側ＩＦ３１０から受信したシグナリングデータ及びユーザデータについては、Ｌ２処理部４００、ＩＰ処理部３８０、Ｌ４処理部３７０でそれぞれ規定の処理が行われた後、移動無線通信プロトコル処理部３３０において移動無線通信制御部３６０の制御に基づき規定の処理が行われる。

【００２９】

また、移動無線通信プロトコル処理部３３０がインターネット側ＩＦ３１０からパケットを送信する場合、以下の手順で処理が行われる。

【００３０】

まずＬ４処理部３７０において、シグナリングデータに対してはＳＣＴＰ処理が、ユーザデータに対してはＵＤＰ処理が行われる。次に、ＩＰ処理部３８０において、送信先の無線基地局６０のオペレータ独自ＩＰアドレスを宛先、無線基地制御局７０自身のオペレータ独自ＩＰアドレスを送信元とする内部ＩＰヘッダが付加される。さらに、自身のグローバルＩＰアドレスを送信元、ＶＰＮゲートウェイ１００のグローバルＩＰアドレスを宛先とする外部ＩＰヘッダでカプセル化される。その際、送信先の無線基地局６０のＳＡ情報がＥＳＰ　ＳＡ情報４２０に含まれている場合には、ＩＰｓｅｃ処理部４１０においてパケットが暗号化され、ＥＳＰヘッダとＥＳＰトレーラが付加される。

【００３１】

加えて、暗号化する際には、パケット内のＬ４ヘッダをコピーしてＥＳＰヘッダの前部に付加する。この理由は、ＬＡＮ２０のＬＡＮデバイスがパケット識別する際に必要となるＬ４ヘッダを閲覧できるようにするためである。

【００３２】

当該パケットはＬ２処理部４１０においてリンク処理が行われた後、インターネット側ＩＦ３１０から送信される。パケット受信時にはこれらの逆の処理が行われる。受信パケットにＥＳＰヘッダとＥＳＰトレーラが含まれる場合には、ＩＰｓｅｃ処理部４１０においてパケットの復号化が行われる。もし正しく復号できない場合には当該パケットは廃棄される。

【００３３】

ＩＰトランスポート処理部４３０が送受信するパケットのフォーマットは、例えば図７の（ｂ）に示すように構成される。図示するように、パケットは外部ＩＰヘッダ８０１、Ｌ４ヘッダ８３３、ＥＳＰヘッダ８１１、内部ＩＰヘッダ８２１、Ｌ４ヘッダ８３１、ペイロード８４１、ＥＳＰトレーラ８５１から構成される。

【００３４】

図１に示した無線基地局６０は、例えば図４に示すような構成を備えている。ここでは、無線基地局６０を例にとって説明するが、無線基地局６１～６３も同様の構成を備えている。

【００３５】

具体的には、無線基地局６０は、ＬＡＮ側ＩＦ５００と無線側ＩＦ５１０の２つのインタフェースを有し、Ｌ２処理部５２０、移動無線通信プロトコル処理部５３０、移動無線通信制御部５６０、ＩＰトランスポート処理部６３０、Ｅｔｈｅｒｎｅｔ(R)処理部６００を備えて構成される。このうち、移動無線通信プロトコル処理部５３０の内部には、シグナリング処理部５４０と、ユーザデータ処理部５５０が備えられる。ＩＰトランスポート処理部６３０には、Ｌ４処理部５７０、ＩＰ処理部５８０と、ＩＰｓｅｃ処理部６１０が備えられる。

【００３６】

ＩＰｓｅｃ処理部６１０はＥＳＰ　ＳＡ情報６２０を保持する。これらの各処理部における基本的な処理を以下に示す。

【００３７】

無線側ＩＦ５１０から受信したシグナリングデータ及びユーザデータは、Ｌ２処理部５２０においてリンク処理が行われた後、ＬＡＮ側ＩＦ５００から受信したシグナリングデータ及びユーザデータについては、Ｅｔｈｅｒｎｅｔ(R)処理部６００、ＩＰ処理部５８

０、Ｌ４処理部５７０においてそれぞれ規定の処理が行われた後、移動無線通信プロトコル処理部５３０において移動無線通信制御部５６０の制御に基づき、規定の処理が行われる。

【００３８】

また、移動無線通信プロトコル処理部５３０が、ＬＡＮ側ＩＦ５００からパケットを送信する場合、以下の手順で処理が行われる。

【００３９】

まず、Ｌ４処理部５７０においてシグナリングデータにはＳＣＴＰ処理を、ユーザデータにはＵＤＰ処理を行う。ＩＰ処理部５８０において送信先の無線基地制御局７０のオペレータ独自ＩＰアドレスを宛先、無線基地局６０自身のオペレータ独自ＩＰアドレスを送信元とする内部ＩＰヘッダが付加される。また、送信元としては自身のプライベートＩＰアドレス、宛先としてはＶＰＮゲートウェイ１００のプライベートＩＰアドレスとする外部ＩＰヘッダによるカプセル化も行われる。

【００４０】

その場合、送信先の無線基地局６０のＳＡ情報がＥＳＰ　ＳＡ情報６２０に含まれている場合には、ＩＰｓｅｃ処理部６１０がパケットの暗号化を行い、ＥＳＰヘッダとＥＳＰトレーラが付加される。加えて、暗号化する際に、Ｌ４ヘッダをコピーしてＥＳＰヘッダの前部に付加する。

【００４１】

当該パケットはＥｔｈｅｒｎｅｔ(R)処理部６００においてリンク処理された後、ＬＡＮ側ＩＦ５００から送信される。パケットを受信した場合はこの逆の処理が行われる。もし受信したパケットがＥＳＰヘッダとＥＳＰトレーラを含む場合は、ＩＰｓｅｃ処理部６１０においてパケットの復号化が行われる。正しく復号化できない場合には当該パケットは廃棄される。

【００４２】

ＩＰトランスポート処理部６３０が送受信するパケットのフォーマットは、例えば図７の（ａ）に示すように構成される。図示するように、パケットは外部ＩＰヘッダ８００、Ｌ４ヘッダ８３２、ＥＳＰヘッダ８１０、内部ＩＰヘッダ８２０、Ｌ４ヘッダ８３０、ペイロード８４０、ＥＳＰトレーラ８５０から構成される。

【００４３】

図１に示したＶＰＮゲートウェイ１００は例えば図５に示すような構成を備えている。

【００４４】

具体的には、ＶＰＮゲートウェイ１００は、Ｇｌｏｂａｌ　ＩＰ　ＩＦ７５０及びＰｒｉｖａｔｅ　ＩＰ　ＩＦ７００、Ｅｔｈｅｒｎｅｔ(R)処理部７１０、７４０、トンネル転送処理部７２０、ＩＰｓｅｃ処理部７６０から構成される。このうち、トンネル転送処理部７２０は経路制御情報７３０を保持し、ＩＰｓｅｃ処理部７６０はＥＳＰ　ＳＡ情報７７０を保持する。

【００４５】

図８～１４を参照して、本発明の第１の実施例に係る移動通信システムを構成するＶＰＮゲートウェイ１００の動作内容について詳細に説明する。例えば、経路制御情報７３０は図８に示すような転送テーブル９００から構成される。ここでは、転送テーブル９００には、１つの無線基地制御局に関するグローバルアドレスとオペレータ独自アドレス、４つの無線基地局に関するプライベートアドレスとオペレータ独自アドレスが登録されている例を示している。

【００４６】

図９はＶＰＮゲートウェイ１００の全体の処理フローを示している。

【００４７】

ＶＰＮゲートウェイ１００は、受信したパケットの外部ＩＰヘッダ内の送信元ＩＰアドレスがグローバルアドレスかプライベートアドレスかの判定を行う（ステップＡ－１）。プライベートアドレスの場合、受信パケットの種別の識別を行う（ステップＡ－２）。

【００４８】
受信パケットが帯域制御応答である場合はＱｏＳシグナリング処理を（ステップＡ－６）、アドレス通知である場合はアドレス通知パケット処理を（ステップＡ－５）行う。これらの処理の詳細については後述する。

【００４９】
受信したパケットがＩＫＥパケットである場合は送信元ＩＰアドレスで転送テーブル９００のプライベートアドレスを検索する（ステップＡ－４）。上記以外の場合は後述するＩＰｓｅｃパケット処理を行う（ステップＡ－３）。

【００５０】
ステップＡ－４において該当するエントリが存在するかどうかを判別し（ステップＡ－７）、存在する場合、後述するＩＫＥパケット転送処理を行い（ステップＡ－８）、該当するエントリが存在しなければ、受信パケットを廃棄する（ステップＡ－９）。

【００５１】
一方、ステップＡ－１において外部ＩＰヘッダ内の送信元ＩＰアドレスがグローバルアドレスの場合、受信パケットの種別の識別を行う（ステップＢ－１）。受信パケットがＩＫＥパケットである場合は送信元ＩＰアドレスで転送テーブル９００のグローバルアドレスを検索し（ステップＢ－３）、該当するエントリが存在するかを判定する（ステップＢ－４）。

【００５２】
受信パケットがＩＫＥパケット以外の場合は後述するＩＰｓｅｃパケット処理を行う（ステップＢ－２）。

【００５３】
ステップＢ－４において該当するエントリが存在する場合、後述するＩＫＥパケット転送処理を行い（ステップＢ－５）、該当するエントリが存在しない場合は、受信パケットを廃棄する（ステップＢ－６）。

【００５４】
図１０に、図９のステップＡ－５におけるアドレス通知パケット処理のフローを示す。この場合、送信元ＩＰアドレスで転送テーブル９００のプライベートアドレスを検索し（ステップＣ－１）、該当するエントリが存在するかどうかを判別する（ステップＣ－２）。

【００５５】
該当するエントリが存在しない場合は、転送テーブル９００に新たなエントリを追加し（ステップＣ－３）、処理を正常に完了したことを示すアドレス通知応答を送信する（ステップＣ－４）。該当するエントリが存在する場合はエラーを含むアドレス通知応答を返送する（ステップＣ－５）。

【００５６】
図１１にＶＰＮゲートウェイ１００によるＳＡ情報の追加／削除処理のフローを示す。この場合、まず要求が追加か削除かの判定を行う（ステップＤ－１）。

【００５７】
追加要求である場合、メッセージ内に含まれるＩＰアドレス、ＩＰｓｅｃプロトコル種別及びＳＰＩ(Security Parameter Index)のすべてが同一であるエントリが存在するかをチェックする（ステップＤ－２）。該当するエントリが存在しない場合、ＳＡ情報のエントリを新たに追加し（ステップＤ－３）、ＳＡ情報追加応答を返信する（ステップＤ－４）。ステップＤ－２において該当するエントリが存在する場合は、ＳＡ情報追加応答（エラー）を返信する（ステップＤ－５）。

【００５８】
削除要求である場合、追加処理と同様にメッセージ内の情報と同一のエントリが存在するかをチェックする（ステップＤ－６）。該当するエントリが存在する場合、ＳＡ情報のエントリを削除し（ステップＤ－７）、ＳＡ情報削除応答を返信する（ステップＤ－８）。ステップＤ－６において該当するエントリが存在しない場合、ＳＡ情報削除応答（エラ

ー）を返信する（ステップＤ－９）。

【００５９】

図１２に、図９のステップＡ－３、Ｂ－２におけるＶＰＮゲートウェイ１００によるＩＰｓｅｃパケット処理のフローを示す。

【００６０】

この場合、まずパケットを受信したＩＦの判定を行う（ステップＥ－１）。

【００６１】

プライベートＩＦでパケットを受信した場合、ＥＳＰヘッダ内のＳＰＩでＳＡ情報を検索してマッチするエントリが存在するかを判定する（ステップＥ－２、Ｅ－３）。

【００６２】

該当するエントリが存在しない場合はパケットを廃棄する（ステップＥ－４）。該当するエントリが存在する場合、該当のＳＡ情報に基づきパケットの復号化を行い（ステップＥ－５）、内部ＩＰヘッダ及びＬ４ヘッダの情報でＳＡ情報の該当するエントリを検索してマッチするエントリが存在するかを判定する（ステップＥ－６、Ｅ－７）。該当するエントリが存在しない場合はパケットを廃棄する（ステップＥ－８）。

【００６３】

該当するエントリが存在する場合、該当するＳＡ情報に基づき暗号化を行い（ステップＥ－９）、ＳＡ情報のトンネル終端先ＩＰアドレスを宛先とするＩＰヘッダに置き換えて、カプセル化転送を行う（ステップＥ－１０）。

【００６４】

一方、グローバルＩＦでパケットを受信した場合、ＥＳＰヘッダ内のＳＰＩでＳＡ情報を検索しマッチするエントリが存在するかを判定する（ステップＥ－１１、Ｅ－１２）。

【００６５】

該当するエントリが存在しない場合はパケットを廃棄する（ステップＥ－１３）。該当するエントリが存在する場合は、該当するＳＡ情報に基づきパケットの復号化を行い（ステップＥ－１４）、パケット種別をチェックする（ステップＥ－１５）。

【００６６】

ＱｏＳシグナリングの場合、後述するＱｏＳシグナリング処理を行い（ステップＥ－１６）、ＳＡ情報追加／削除要求である場合、図１１に示したＳＡ情報追加／削除処理を行う（ステップＥ－１７）。

【００６７】

ステップＥ－１５においてパケット種別が上記以外の場合、内部ＩＰヘッダ及びＬ４ヘッダの情報でＳＡ情報の該当するエントリを検索し、マッチするエントリが存在するかを判定する（ステップＥ－１８、Ｅ－１９）。

【００６８】

該当するエントリが存在しない場合はパケットを廃棄する（ステップＥ－２０）。該当するエントリが存在する場合、該当するＳＡ情報に基づきパケットの暗号化を行い（ステップＥ－２１）、ＳＡ情報のトンネル終端先ＩＰアドレスを宛先とする外部ＩＰヘッダに置き換えて、カプセル化転送を行う（ステップＥ－２２）。

【００６９】

図１３に図９のステップＡ－８、Ｂ－５におけるＶＰＮゲートウェイ１００によるＩＫＥパケット転送処理のフローを示す。

【００７０】

この場合、まずパケットを受信したインタフェース（ＩＦ）の判定を行う（ステップＦ－１）。

【００７１】

受信ＩＦがプライベートＩＦである場合、送信元ＩＰアドレスで転送テーブル９００のプライベートアドレスを検索し、マッチするエントリが存在するかを判定する（ステップＦ－２、Ｆ－３）。

【００７２】

該当するエントリが存在しない場合は、パケットを廃棄する（ステップＦ－４）。

【００７３】

該当するエントリが存在する場合、外部ＩＰヘッダを削除し（ステップＦ－５）、該当するエントリに記載のグローバルアドレスを宛先とするＩＰヘッダを付加して、カプセル化転送を行う（ステップＦ－６）。

【００７４】

一方、ステップＦ－１において受信ＩＦがグローバルＩＦである場合、送信元ＩＰアドレスで転送テーブル９００のグローバルアドレスを検索し、マッチするエントリが存在するかを判定する（ステップＦ－７、Ｆ－８）。

【００７５】

該当するエントリが存在しない場合はパケットを廃棄する（ステップＦ－９）。該当するエントリが存在する場合、内部ＩＰヘッダ内の宛先ＩＰアドレスで転送テーブル９００の無線基地局のオペレータ独自アドレスを検索し、マッチするエントリが存在するかを判定する（ステップＦ－１０、Ｆ－１１）。

【００７６】

該当するエントリが存在しない場合はパケットを廃棄する（ステップＦ－１２）。該当するエントリが存在する場合、外部ＩＰヘッダを削除し（ステップＦ－１３）、該当するエントリに記載のプライベートアドレスを宛先とするＩＰヘッダを付加して、カプセル化転送を行う（ステップＦ－１４）。

【００７７】

図１４に、図９のステップＡ－６におけるＶＰＮゲートウェイ１００によるＱｏＳシグナリング処理の動作フローを示す。

【００７８】

この場合も、まずパケットの受信ＩＦの判定を行う（ステップＧ－１）。

【００７９】

受信ＩＦがプライベートＩＦの場合、受信した帯域制御応答（ＣＯＰＳ　Ｄｅｃｉｓｉｏｎ）メッセージ内部の受付判定結果をチェックする（ステップＧ－２）。

【００８０】

判定結果が「ＮＧ」の場合は判定結果とトラヒック情報を含むＱｏＳシグナリングを作成し、無線基地制御局７０に送信する（ステップＧ－３）。

【００８１】

判定結果が「ＯＫ」の場合、帯域制御応答メッセージで通知されたトラヒック情報及び帯域制御情報を抽出し（ステップＧ－４）、抽出した各種情報をＱｏＳシグナリングに含めて、無線基地制御局７０に送信する（ステップＧ－５）。

【００８２】

一方、ステップＧ－１において受信ＩＦがグローバルＩＦの場合、ＱｏＳシグナリング内のトラヒック情報を抽出し（ステップＧ－６）、抽出したトラヒック情報を含む帯域制御要求（ＣＯＰＳ　Ｒｅｑｕｅｓｔ）メッセージを作成し、ポリシーサーバ２００に送信する（ステップＧ－７）。

【００８３】

ポリシーサーバ２００は、例えば図６に示すような構成を備えている。具体的に説明すると、ポリシーサーバ２００は、ＬＡＮ　ＩＦ１３００、Ｅｔｈｅｒｎｅｔ(R)処理部１３１０、ＩＰ処理部１３２０、Ｌ４処理部１３３０、制御プロトコル処理部１３４０、帯域制御処理部１３５０を備えて構成される。制御プロトコル処理部１３４０は、ＣＯＰＳ処理部１３６０とＳＮＭＰ処理部１３７０を有する。これらの各処理部の基本的な処理内容を以下に示す。

【００８４】

ＳＮＭＰ処理部１３７０は、ＬＡＮ　ＩＦ１３００、Ｅｔｈｅｒｎｅｔ(R)処理部１３１０、ＩＰ処理部１３２０、Ｌ４処理部１３３０を経て受信した、ＬＡＮ２０のＬＡＮデバイスからのＳＮＭＰメッセージを受信し、メッセージ内の帯域制御状態情報を抽出し、

帯域制御処理部１３５０に通知する。

【００８５】

帯域制御処理部１３５０は、これらの情報を収集／管理し、ＬＡＮ２０内の帯域制御状態を集中管理する。

【００８６】

ＣＯＰＳ処理部１３６０は、帯域制御処理部１３５０からの指示を受けることにより、ＬＡＮデバイスに対して帯域制御情報及びトラヒック情報をＣＯＰ　Ｄｅｃｉｓｉｏｎメッセージで通知する。

【００８７】

また、ＶＰＮゲートウェイ１００から送られた帯域制御要求メッセージは、ＬＡＮ　ＩＦ１３００、Ｅｔｈｅｒｎｅｔ(R)処理部１３１０、ＩＰ処理部１３２０、Ｌ４処理部１３３０を経てＣＯＰＳ処理部１３６０に送られ、ＣＯＰＳ処理部１３６０が帯域制御要求メッセージ内のトラヒック情報と帯域制御情報を抽出し、帯域制御処理部１３５０に通知する。

【００８８】

これを受けた帯域制御処理部１３５０は、収集した帯域制御情報に基づき受付判定を行い、許可した帯域制御情報と共に判定結果をＣＯＰＳ処理部１３６０に通知する。判定結果が「ＯＫ」であった場合には、ＣＯＰＳ処理部１３６０は判定結果と許可された帯域制御情報を含む帯域制御応答メッセージを生成し、ＶＰＮゲートウェイ１００に送信する。また、ＬＡＮ２０の移動通信トラヒックの経路上のＬＡＮデバイスあるいはすべてのＬＡＮデバイスにトラヒック情報と帯域制御情報を配信する。

【００８９】

図１５を参照して、本発明の第１の実施形態に係る移動通信システムにおける無線基地制御局７０と無線基地局６０間で通信経路を確立するための動作シーケンスについて詳細に説明する。図１５においては、無線基地局６０の送受信パケットシーケンス１０００、ＶＰＮゲートウェイ１００の送受信パケットシーケンス１０１０、及び無線基地制御局７０の送受信パケットシーケンス１０２０を示している。

【００９０】

本実施例では、ＶＰＮゲートウェイ１００と無線基地制御局７０間には予めＳＡが確立されており、無線基地局６０とＶＰＮゲートウェイ１００間でＳＡを確立する際に必要となる事前共有鍵は、無線基地制御局７０と無線基地局６０に予め設定されているものとする。

【００９１】

以下では、より詳細な動作シーケンスを説明する。無線基地局６０は起動すると、ＤＨＣＰ(Dynamic Host Configuration Protocol)により自身のプライベートＩＰアドレスを取得した後、ＤＮＳ(Domain Name Server)を利用してＶＰＮゲートウェイ１００のプライベートＩＰアドレスを取得する。

【００９２】

その後、ＶＰＮゲートウェイ１００に対して、無線基地制御局７０のグローバルアドレスとオペレータ独自アドレス、無線基地局６０のプライベートアドレスとオペレータ独自アドレスをアドレス通知メッセージで通知する。

【００９３】

ＶＰＮゲートウェイ１００はこれを受けて、転送テーブル９００に通知されたアドレス群を設定し、設定したエントリを削除するためのタイマをセットすると共に、アドレス通知応答メッセージを返信する（ステップ（１））。

【００９４】

返信メッセージを受けた無線基地局６０は、ＶＰＮゲートウェイ１００とのＩＳＡＫＭＰ　ＳＡ及び上りと下りの２つのＩＰｓｅｃ　ＳＡを確立する（ステップ（２）～（４））。その場合、ＶＰＮゲートウェイ１００は無線基地局６０から受信したＩＫＥパケットのアドレス変換のみを行い、無線基地制御局７０に転送する。

【００９５】
逆に、無線基地制御局７０から受信したＩＫＥパケットもアドレス変換のみを行い、無線基地局６０に転送する。
【００９６】
このようにして無線基地制御局７０と無線基地局６０間でＳＡが確立されると、無線基地制御局７０はすべてのＳＡ情報をＳＡ情報追加メッセージにてＶＰＮゲートウェイ１００に通知する。
【００９７】
ＶＰＮゲートウェイ１００は、受信したＳＡ情報をデータベースに追加し、ステップ（１）でセットしたタイマを解除すると共に、ＳＡ情報追加応答メッセージにて設定が完了したことを通知する（ステップ（５））。
【００９８】
これにより、ＶＰＮゲートウェイ１００と無線基地局６０間ではＩＰｓｅｃによる暗号化通信が可能となり、ＶＰＮゲートウェイ１００を介することで無線基地局６０と無線基地制御局７０はＩＰｓｅｃ　ＳＡによる暗号化通信を開始できる（ステップ（６））。
【００９９】
もし、ＶＰＮゲートウェイ１００がＳＡ情報追加メッセージを受信せずに、タイマがタイムアウトした際には、速やかに追加した転送テーブル９００のエントリを削除する。
【０１００】
図１６及び図１７を参照して、本発明の第１の実施例に係る移動通信システムにおける無線基地制御局７０と無線基地局６０間のユーザトラヒックに対する帯域制御動作シーケンスを詳細に説明する。
【０１０１】
図１６に端末が着呼した場合の動作シーケンスを示す。図１６においては、無線基地制御局７０のパケット送受信シーケンス１１００、ＶＰＮゲートウェイ１００のパケット送受信シーケンス１１１０、ポリシーサーバ２００のパケット送受信シーケンス１１２０、無線基地局６０のパケット送受信シーケンス１１３０、移動端末８０のパケット送受信シーケンス１１４０を示している。
【０１０２】
無線基地制御局７０は、移動通信コア網３０からのページング要求メッセージを受信すると（ステップ（１））、移動端末８０のページングを行い（ステップ（２））、これに対して移動端末８０はＲＲＣコネクション要求を無線基地制御局７０に送信し（ステップ（３））、これを受信した無線基地制御局７０は無線基地局６０に対して無線リンク設定要求を送信する（ステップ（４））。
【０１０３】
無線リンクの設定を完了すると、無線基地局６０は、無線基地制御局７０に無線リンク設定応答を返送し（ステップ（５））、無線基地制御局７０は、ＲＲＣコネクション設定を移動端末８０に送信する（ステップ（６））。
【０１０４】
これを受けた移動端末８０は、各種パラメータを設定した後、ＲＲＣコネクション設定完了を無線基地制御局７０に送信する（ステップ（７））。その後、移動端末８０は、セルアップデータメッセージにより位置登録を行う（ステップ（８））。
【０１０５】
これを受けた無線基地制御局７０は、セルアップデート確認メッセージで返信すると共に（ステップ（９））、ページング応答を移動通信コア網３０に返送する（ステップ（１０））。この後、無線基地制御局７０は、移動通信コア網３０から送られた無線アクセスベアラ割当要求メッセージを受信し（ステップ（１１））、無線ベアラ確立要求メッセージに含まれるＱｏＳ情報に基づき、無線リンクの設定を行う。
【０１０６】
具体的には、無線基地制御局７０は、無線基地局６０に無線リンク設定要求を送信し（

ステップ（１２））、無線基地局６０は無線リンクの設定が完了すると無線リンク設定応答を返信する（ステップ（１３））。

【０１０７】

これを受けた無線基地制御局７０は、要求されたＱｏＳの情報を含むＱｏＳシグナリングを生成し、無線基地局６０に送信する（ステップ（１４））。

【０１０８】

ＶＰＮゲートウェイは、このＱｏＳシグナリングをインターセプトし、ＱｏＳシグナリングから抽出したトラヒック情報を含む帯域制御要求メッセージをポリシーサーバ２００に送信する（ステップ（１５））。ここでのＱｏＳシグナリングとは、例えばＩＰ－ＡＬＣＡＰ(Access Link Control Application Part)シグナリングである。

【０１０９】

ポリシーサーバ２００は、収集した帯域制御状態情報と帯域制御要求メッセージで通知されたトラヒック情報に基づき受付判定を行い、受付判定結果及び許可した帯域制御情報を帯域制御応答メッセージに含めてＶＰＮゲートウェイ１００に送信する通知する（ステップ（１６））。

【０１１０】

ＶＰＮゲートウェイ１００は、帯域制御応答メッセージに含まれる受付判定結果と帯域制御情報をＱｏＳシグナリングに含めて無線基地制御局７０に送信する（ステップ（１７））。本実施例ではポリシーサーバ２００が受付許可と判定した例を示している。

【０１１１】

受付を許可した場合、ポリシーサーバ２００は、ＬＡＮ２０のＬＡＮデバイスにトラヒック情報と帯域制御情報の配布も行う（図示せず）。ＬＡＮ内の帯域確保が完了すると、無線基地制御局７０は、移動端末８０に無線ベアラ設定を送信する（ステップ（１８））。

【０１１２】

これを受信した移動端末８０は、無線ベアラの設定を行い、完了すると無線ベアラ設定完了を返信する（ステップ（１９））。この後、移動端末８０は、無線基地制御局７０及び移動通信コア網３０を経由してデータ通信を行う。ＬＡＮ２０の移動通信トラヒックの経路上にあるＬＡＮデバイスは、通知されたトラヒック情報と帯域制御情報に基づいてユーザデータトラヒックの帯域制御が行う。

【０１１３】

図１７に移動端末８０が発呼した場合の動作シーケンスを示す。図１７においては、無線基地制御局７０のパケット送受信シーケンス１２００、ＶＰＮゲートウェイ１００のパケット送受信シーケンス１２１０、ポリシーサーバ２００のパケット送受信シーケンス１２２０、無線基地局６０のパケット送受信シーケンス１２３０、移動端末８０のパケット送受信シーケンス１２４０を示している。

【０１１４】

移動端末８０は、データの送信要求をトリガとしてＲＲＣコネクション要求を無線基地制御局７０に送信する（ステップ（１））。これを受信した無線基地制御局７０は、無線基地局６０へ無線リンク設定要求を送信する（ステップ（２））。無線基地局６０は、無線リンクの設定を有効化し、無線基地制御局７０に無線リンク設定応答を返す（ステップ（３））。

【０１１５】

無線基地局６０からの無線リンク設定応答を受信した無線基地制御局７０は、ＲＲＣコネクション設定を移動端末８０に送信し（ステップ（４））、移動端末８０は、無線リンクの設定が完了すると、ＲＲＣコネクション設定完了を無線基地制御局７０に送信する（ステップ（５））。また、移動端末８０は、利用するサービスのＱｏＳ情報を含むアクティベイトＰＤＰコンテキスト要求を移動通信コア網３０に送信する（ステップ（６））。

【０１１６】

これを受けて、移動通信コア網３０は、無線アクセスベアラ割当要求を無線基地制御局

７０に送信する（ステップ（７））。無線基地制御局７０は、無線アクセスベアラ割当要求に含まれるＱｏＳ情報に基づき、無線リンクの設定を行う。具体的には、無線基地制御局７０は、無線基地局６０に無線リンク設定要求を送信し（ステップ（８））、無線基地局６０が無線リンクの設定を完了すると、無線リンク設定応答を返送する（ステップ（９））。

【０１１７】

これを受けて、無線基地制御局７０は、ＱｏＳ情報を含むＱｏＳシグナリングを生成し、無線基地局６０宛に送信する（ステップ（１０））。ＶＰＮゲートウェイ１００は、このＱｏＳシグナリングをインターセプトし、受信したＱｏＳシグナリングから抽出したＱｏＳ情報を含む帯域制御要求メッセージをポリシーサーバ２００に送信する（ステップ（１１））。

【０１１８】

ポリシーサーバ２００は、収集した帯域制御状態情報と帯域制御要求メッセージで通知されたＱｏＳ情報に基づき受付判定を行い、受付判定結果及び許可した帯域制御情報を帯域制御応答メッセージに含めてＶＰＮゲートウェイ１００に送信する通知する（ステップ（１２））。

【０１１９】

ＶＰＮゲートウェイ１００は、帯域制御応答メッセージに含まれる受付判定結果と帯域制御情報をＱｏＳシグナリングに含めて無線基地制御局７０に送信する（ステップ（１３））。本実施例でもポリシーサーバ２００が受付許可と判定した例を示している。

【０１２０】

受付を許可した場合、ポリシーサーバ２００は、ＬＡＮ２０のＬＡＮデバイスにトラヒック情報と帯域制御情報を配布する（図示せず）。その後、無線基地制御局７０は移動端末８０に対して無線ベアラ設定を通知する（ステップ（１４））。

【０１２１】

移動端末８０は、無線リンクの設定を行い、完了すると無線ベアラ設定完了を無線基地制御局７０に通知する（ステップ（１５））。これを受けて、無線基地制御局７０は、無線アクセスベアラ割当応答を移動通信コア網３０に返送する（ステップ（１６））。

【０１２２】

移動端末８０は、移動通信コア網３０からアクティベイトＰＤＰコンテキスト受付を受信する（ステップ（１７））と、無線基地制御局７０及び移動通信コア網３０を経由してデータ通信を行う。ＬＡＮ２０の移動通信トラヒックの経路上にあるＬＡＮデバイスは通知されたトラヒック情報と帯域制御情報に基づいてユーザデータトラヒックの帯域制御を行う。

【０１２３】

図１及び２に示すネットワーク構成図を用いて本発明の第２の実施例に係わる移動通信システムを説明する。この第２の実施例では、無線基地制御局７０は、例えば図１８に示す構成を備えている。

【０１２４】

第１の実施形態での無線基地制御局７０の構成と比較して、本第２の実施例では、ＩＰトランスポート処理部４３０がＩＰ処理部３８０、Ｌ４処理部３７０、ＩＰｓｅｃ処理部４１０に加えて、認証処理部４５０を備えている。

【０１２５】

認証処理部４５０は、無線基地局６０～６３との間で認証を行うと共に、認証が成功した場合には、鍵交換メカニズムを用いて事前共有鍵の生成も行う。無線基地制御局７０は、ＳＡが確立すると、生成した事前共有鍵をＶＰＮゲートウェイ１００に通知する。ＶＰＮゲートウェイ１００は、この事前共有鍵を用いて無線基地局６０～６３と間でＩＰｓｅｃ　ＳＡの確立を行う。

【０１２６】

無線基地局６０は、例えば図１９に示す構成を備える。ここでの実施例では無線基地局

６０について説明するが、無線基地局６１～６３についても同様の構成を備えている。第１の実施形態での無線基地局６０の構成と比較して、本実施例では、ＩＰトランスポート処理部６３０がＩＰ処理部５８０、Ｌ４処理部５７０、ＩＰｓｅｃ処理部６１０に加えて、認証処理部６４０を備えている。認証処理部６４０は、無線基地制御局７０との間で認証を行うために、上述した認証処理部４５０と同様の機能を有する。

【０１２７】

図２０～２２を用いてＶＰＮゲートウェイ１００の動作フローを説明する。

【０１２８】

図２０に全体の処理フローを示す。まず、パケットを受信することで処理を開始し、受信したパケットの種別を判定する（ステップＨ－１）。受信したパケットがＩＰｓｅｃパケットであった場合、後述するＩＰｓｅｃパケット処理を行う（ステップＨ－２）。ＩＫＥパケットであった場合、ＲＦＣ２４０９で規定されているＩＫＥパケット処理を行う（ステップＨ－３）。認証パケットであった場合、後述する認証パケット転送処理を行う（ステップＨ－４）。帯域制御応答メッセージであった場合、ＱｏＳシグナリング処理を行う（ステップＨ－５）。ここでのＱｏＳシグナリング処理は第１の実施形態で示したＱｏＳシグナリング処理と同様である。受信したパケットが上記以外の場合はパケットを廃棄する（ステップＨ－６）。

【０１２９】

図２１に、上記ステップＨ－２におけるＶＰＮゲートウェイ１００のＩＰｓｅｃパケット処理のフローを示す。第１の実施形態で示した図１２のＩＰｓｅｃパケット処理では、グローバルＩＦからパケットを受信し、ＥＳＰヘッダ内のＳＰＩでＳＡ情報を検索した際に、該当するエントリが存在し、且つパケット種別がＳＡ情報追加／削除要求である場合に、ステップＥ－１７でＳＡ情報追加／削除処理を行うようにしていたが、本実施例では、パケット種別がＳＡ情報追加／削除要求ではなく、認証パケットである場合に、ＳＡ情報追加／削除処理の代わりに認証パケット転送処理を行う（ステップＩ－１７）点で第１の実施例と異なる。

【０１３０】

その他のステップについては、図１２と同様であるので、同じステップ番号を付して説明を省略する。

【０１３１】

図２２に図２１のステップＩ－１７における認証パケット転送処理のフローを示す。この場合、まずパケットを受信したＩＦの判定を行う（ステップＪ－１）。

【０１３２】

受信ＩＦがプライベートＩＦの場合、内部ＩＰヘッダのＳＰＩでＳＡ情報を検索し、マッチするエントリが存在するかを判定する（ステップＪ－２、Ｊ－３）。

【０１３３】

該当するエントリが存在しない場合はパケットを廃棄する（ステップＪ－４）。

【０１３４】

該当するエントリが存在する場合、該当するＳＡ情報に基づき復号化を行い（ステップＪ－５）、ＳＡ情報のトンネル終端先のＩＰアドレスでカプセル化して転送する（ステップＪ－６）。

【０１３５】

一方、ステップＪ－１において受信ＩＦがグローバルＩＦの場合、事前共有鍵通知メッセージであるかの判定を行う（ステップＪ－７）。

【０１３６】

事前共有鍵通知メッセージである場合、メッセージ内の事前共有鍵を抽出し、ＩＰｓｅｃ処理部７６０に通知する（ステップＪ－８）。

【０１３７】

それ以外の場合、内部ＩＰヘッダの宛先ＩＰアドレスで転送テーブル９００を検索し、マッチするエントリが存在するかを判定する（ステップＪ－９、Ｊ－１０）。

【０１３８】
該当するエントリが存在しない場合はパケットを廃棄する（ステップＪ－１１）。該当するエントリが存在する場合は、該当するエントリのプライベートアドレスでカプセル化して転送する（ステップＪ－１２）。

【０１３９】
また、図２３を参照して、本発明の第２の実施例に係る移動通信システムにおける無線基地制御局７０と無線基地局６０間で通信経路を確立するための動作シーケンスを詳細に説明する。

【０１４０】
第２の実施例では、無線基地局６０と無線基地制御局７０間の相互認証で使用する認証鍵が予め設定されており、無線基地制御局７０とＶＰＮゲートウェイ１００の間のＳＡは事前に確立されているものとする。また、ＶＰＮゲートウェイ１００が有する転送テーブル９００も予め設定されているものとする。図２３においては、無線基地局６０のパケット送受信シーケンス１４００、ＶＰＮゲートウェイ１００のパケット送受信シーケンス１４１０、及び無線基地制御局７０のパケット送受信シーケンス１４２０が示されている。

【０１４１】
無線基地局６０は起動すると、事前に設定されている認証鍵を用いて、無線基地制御局７０との間で相互認証を行う（ステップ（１））。ここでの認証方式は、例えば認証鍵を利用したチャレンジ／レスポンス型のワンタイムパスワード方式が利用可能である。

【０１４２】
相互認証が成功した場合、無線基地局６０と無線基地制御局７０において鍵交換メカニズムにより認証鍵から事前共有鍵の生成を行う（ステップ（２））。ここでの鍵交換メカニズムとしては、例えばＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵交換方式が利用可能である。

【０１４３】
鍵の生成が完了すると、無線基地制御局７０はＶＰＮゲートウェイ１００に対して事前共有鍵を通知する（ステップ（３））。

【０１４４】
無線基地局６０は上述した鍵交換メカニズムにより生成した事前共有鍵を用いてＩＳＡＫＭＰ　ＳＡの確立を行う（ステップ（４））。

【０１４５】
ＩＳＡＫＭＰ　ＳＡを確立すると、次にＩＰｓｅｃ　ＳＡ（上り）とＩＰｓｅｃ　ＳＡ（下り）の確立も行う（ステップ（５）、（６））。

【０１４６】
上り／下りの２つのＩＰｓｅｃ　ＳＡが確立すると、無線基地局６０と無線基地制御局７０はＶＰＮゲートウェイ１００を介することで、ＩＰｓｅｃ　ＥＳＰによる暗号化通信が可能となる（ステップ（７））。

【０１４７】
なお、上記の構成において、ＶＰＮゲートウェイ１００、無線基地制御局７０の機能については、ハードウェア的に実現することは勿論として、上記したＶＰＮゲートウェイ１００の機能をソフトウェア的に実現するプログラム（中継ノード用プログラム）、無線基地制御局７０の機能をソフトウェア的に実現する制御プログラム（無線基地制御局用プログラム）を、それぞれＶＰＮゲートウェイ１００、無線基地制御局７０を構成するコンピュータ処理装置上で実行することで実現することができる。これらのプログラムは、磁気ディスク、半導体メモリその他の記録媒体に格納され、その記録媒体からＶＰＮゲートウェイ１００、無線基地制御局７０としてのコンピュータ処理装置にロードされ、コンピュータ処理装置の動作を制御することにより、上述した各機能を実現する。

【０１４８】
以上好ましい実施例をあげて本発明を説明したが、本発明は必ずしも上記実施例に限定されるものではなく、その技術的思想の範囲内において様々に変形して実施することができる。

【図面の簡単な説明】

【０１４９】

【図１】本発明の第１の実施例によるネットワークの全体構成を示すブロック図である。

【図２】本発明の第１の実施例におけるＬＡＮの構成を示すブロック図である。

【図３】本発明の第１の実施例における無線基地制御局の構成を示すブロック図である。

【図４】本発明の第１の実施例における無線基地局の構成を示すブロック図である。

【図５】本発明の第１の実施例におけるＶＰＮゲートウェイの構成を示すブロック図である。

【図６】本発明の第１の実施例におけるポリシーサーバの構成を示すブロック図である。

【図７】本発明の第１の実施例における転送テーブルの構成例を示す図である。

【図８】本発明の第１の実施例におけるパケットフォーマットの構成を示す図である。

【図９】本発明の第１の実施例におけるＶＰＮゲートウェイにおける全体処理を説明するフローチャートである。

【図１０】本発明の第１の実施例におけるＶＰＮゲートウェイのアドレス通知処理を説明するフローチャートである。

【図１１】本発明の第１の実施例におけるＶＰＮゲートウェイのＳＡ情報追加／削除処理を説明するフローチャートである。

【図１２】本発明の第１の実施例におけるＶＰＮゲートウェイのIPｓｅｃパケット処理を説明するフローチャートである。

【図１３】本発明の第１の実施例におけるＶＰＮゲートウェイのＩＫＥパケット処理を説明するフローチャートである。

【図１４】本発明の第１の実施例におけるＶＰＮゲートウェイにおけるＱｏＳシグナリング処理を説明するフローチャートである。

【図１５】本発明の第１の実施例における無線基地制御局と無線基地局間の通信開始シーケンス図である。

【図１６】本発明の第１の実施例における着呼時の帯域制御動作のシーケンス図である。

【図１７】本発明の第１の実施例における発呼時の帯域制御動作のシーケンス図である。

【図１８】本発明の第２の実施例における無線基地制御局の構成を示すブロック図である。

【図１９】本発明の第２の実施例における無線基地局の構成を示すブロック図である。

【図２０】本発明の第２の実施例におけるＶＰＮゲートウェイの全体処理を説明するフローチャートである。

【図２１】本発明の第２の実施例を説明するめのＶＰＮゲートウェイにおけるＩＰｓｅｃパケット処理フロー図である。

【図２２】本発明の第２の実施例におけるＶＰＮゲートウェイの認証パケット転送処理を説明するフローチャートである。

【図２３】本発明の第２の実施例における無線基地制御局と無線基地局間の通信開始シーケンス図である。

【符号の説明】

【０１５０】

１０：インターネット網

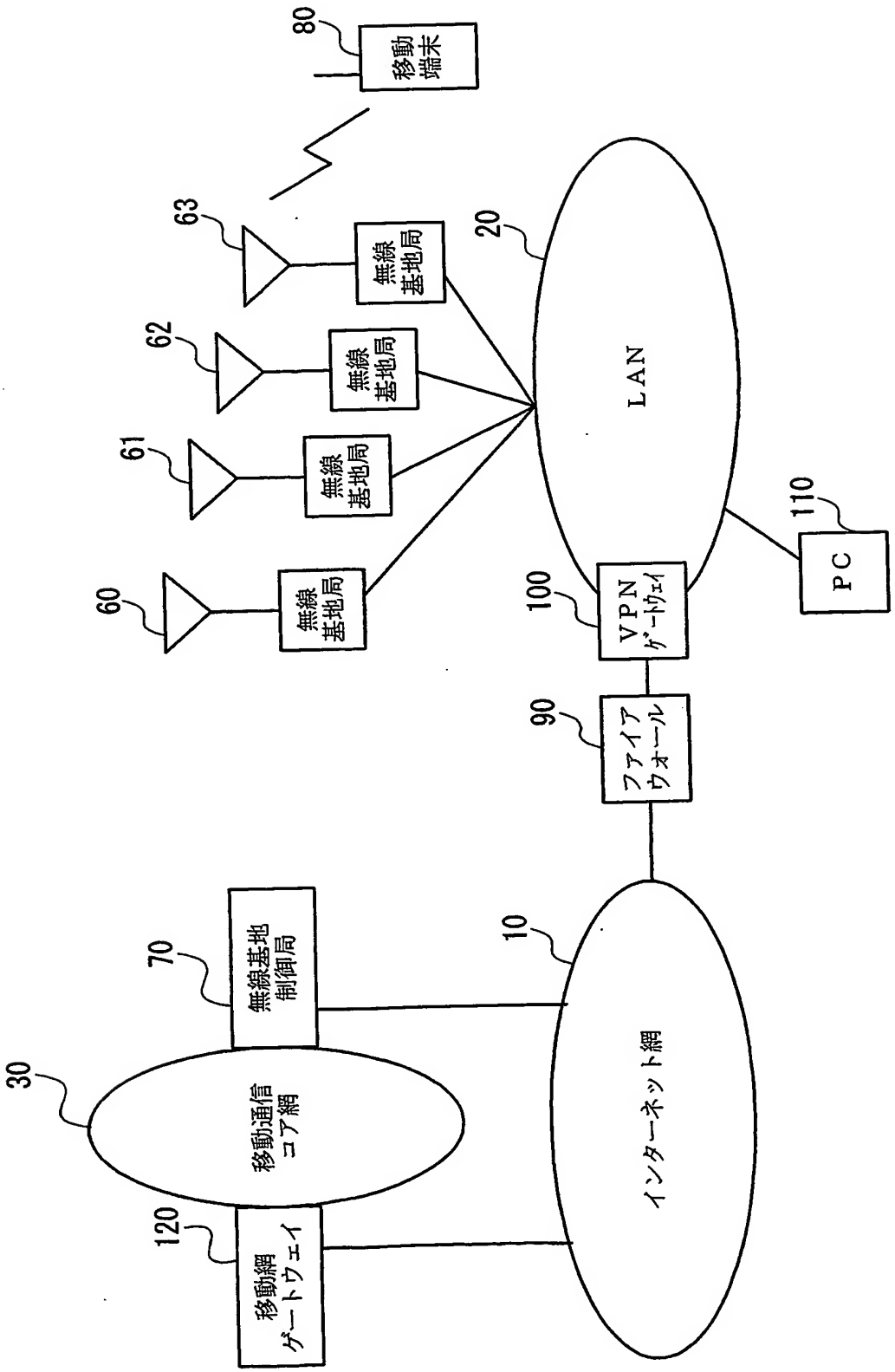
２０：ＬＡＮ

３０：移動通信コア網

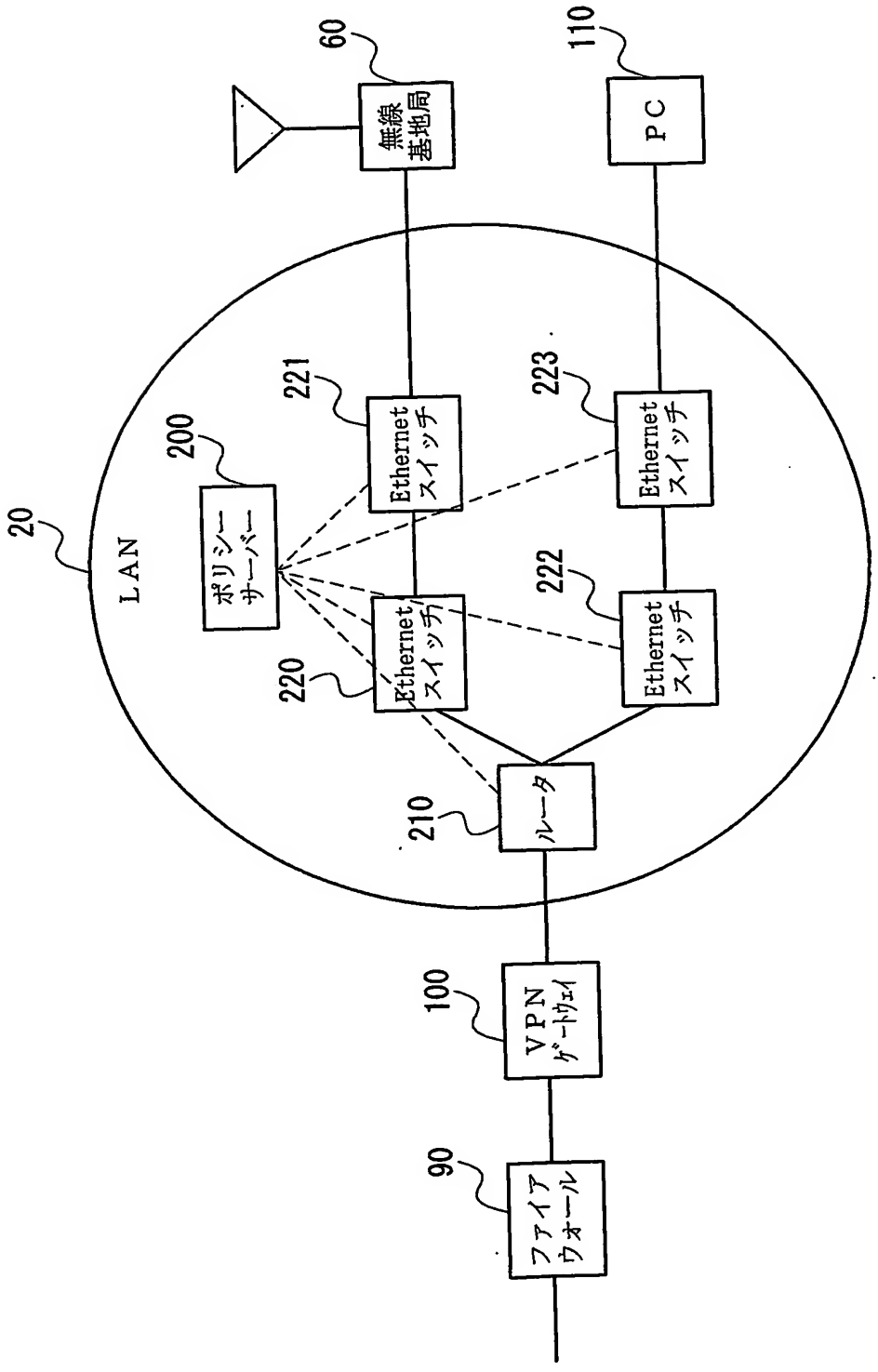
６０、６１、６２、６３：無線基地局
７０：無線基地制御局
８０：移動端末
９０：ファイアウォール
１００：ＶＰＮゲートウェイ
１１０：ＰＣ
１２０：移動網ゲートウェイ
２００：ポリシーサーバ
２１０：ルータ
２２０～２２３：Ｅｔｈｅｒｎｅｔ(R)スイッチ
３００：移動通信コア網側ＩＦ
３１０：インターネット側ＩＦ
３２０、４００、５２０：Ｌ２処理部
３３０、５３０：移動無線通信プロトコル処理部
３４０、５４０：シグナリング処理部
３５０、５５０：ユーザデータ処理部
３６０、５６０：移動無線通信制御部
３７０、５７０：Ｌ４処理部
３８０、５８０：ＩＰ処理部
４１０、６１０、７６０：ＩＰｓｅｃ処理部
４２０、６２０、７７０：ＥＳＰ　ＳＡ情報
４３０、６３０：ＩＰトランスポート処理部
４４０、７８０：帯域制御処理部
４５０、６４０：認証処理部
５００：ＬＡＮ側ＩＦ
５１０：無線側ＩＦ
６００、７１０、７４０：Ｅｔｈｅｒｎｅｔ(R)処理部
７００：プライベートＩＰ　ＩＦ
７２０：トンネル転送処理部
７３０：経路制御情報
７５０：グローバルＩＰ　ＩＦ
８００、８０１：外部ＩＰヘッダ
８１０、８１１：ＥＳＰヘッダ
８２０、８２１：内部ＩＰヘッダ
８３０、８３１：Ｌ４ヘッダ
８４０、８４１：ペイロード
８５０、８５１：ＥＳＰトレーラ
９００：転送テーブル
１０００、１１３０、１２３０、１４００：無線基地局のパケット送受信シーケンス
１０１０、１１１０、１２１０、１４１０：ＶＰＮゲートウェイのパケット送受信シーケンス
１０２０、１１００、１２００、１４２０：無線基地制御局のパケット送受信シーケンス
１１２０、１２２０：ポリシーサーバのパケット送受信シーケンス
１１４０、１２４０：移動端末のパケット送受信シーケンス
１３００：ＬＡＮ　ＩＦ
１３１０：Ｅｔｈｅｒｎｅｔ(R)処理部
１３２０：ＩＰ処理部
１３３０：Ｌ４処理部
１３４０：制御プロトコル処理部

１３５０：帯域制御処理部
１３６０：ＣＯＰＳ処理部
１３７０：ＳＮＭＰ処理部

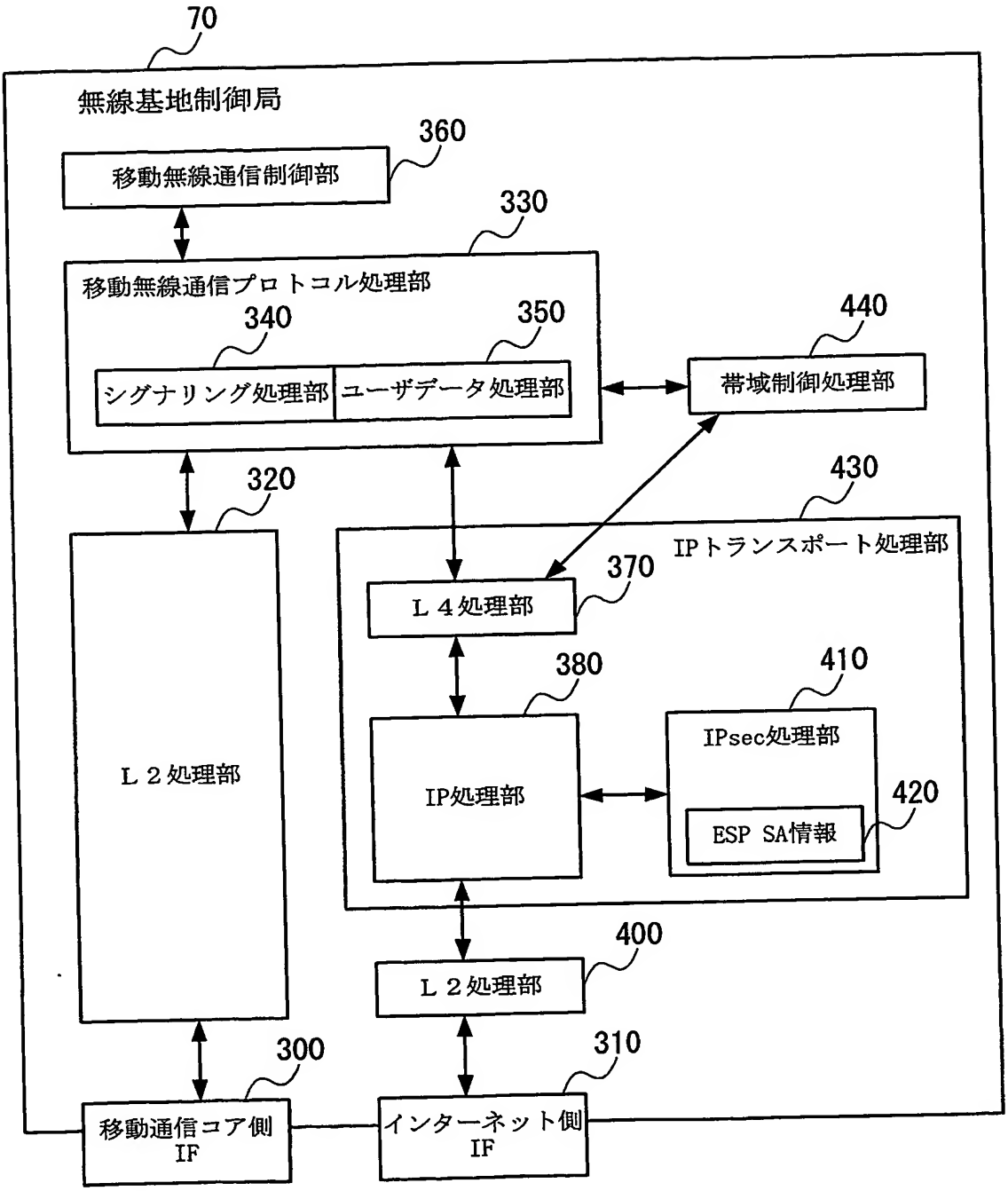
【書類名】図面
【図１】


80
移動端末
63
無線基地局
62
無線基地局
61
無線基地局
60
無線基地局
20
LAN
110
PC
100
VPN ゲートウェイ
90
ファイアウォール
10
インターネット網
70
無線基地制御局
30
移動通信コア網
120
移動網ゲートウェイ

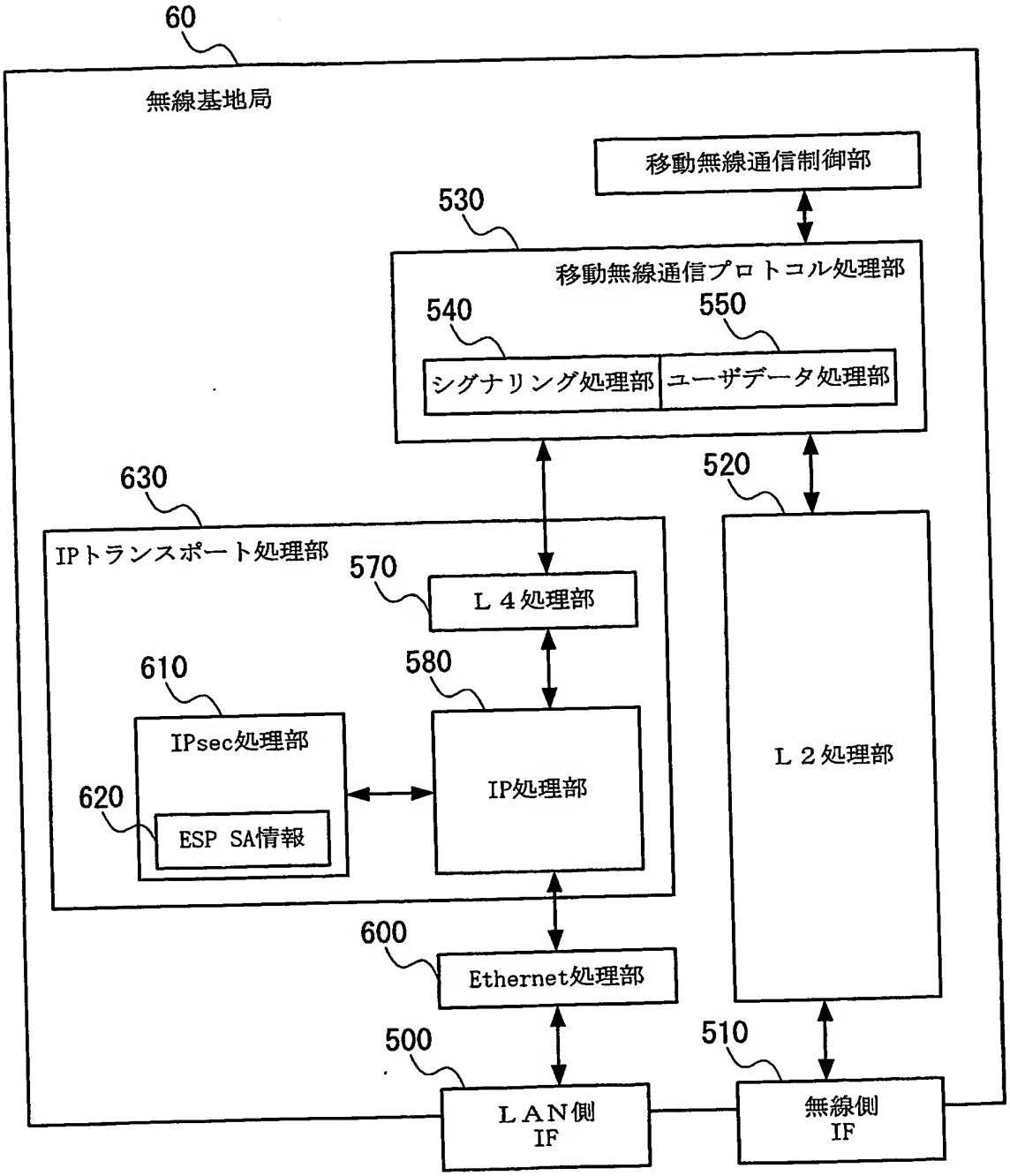
【図２】


60
無線基地局
110
PC
20
LAN
200
ポリシーサーバー
221
Ethernetスイッチ
223
Ethernetスイッチ
222
Ethernetスイッチ
220
Ethernetスイッチ
210
ルータ
100
VPNゲートウェイ
90
ファイアウォール

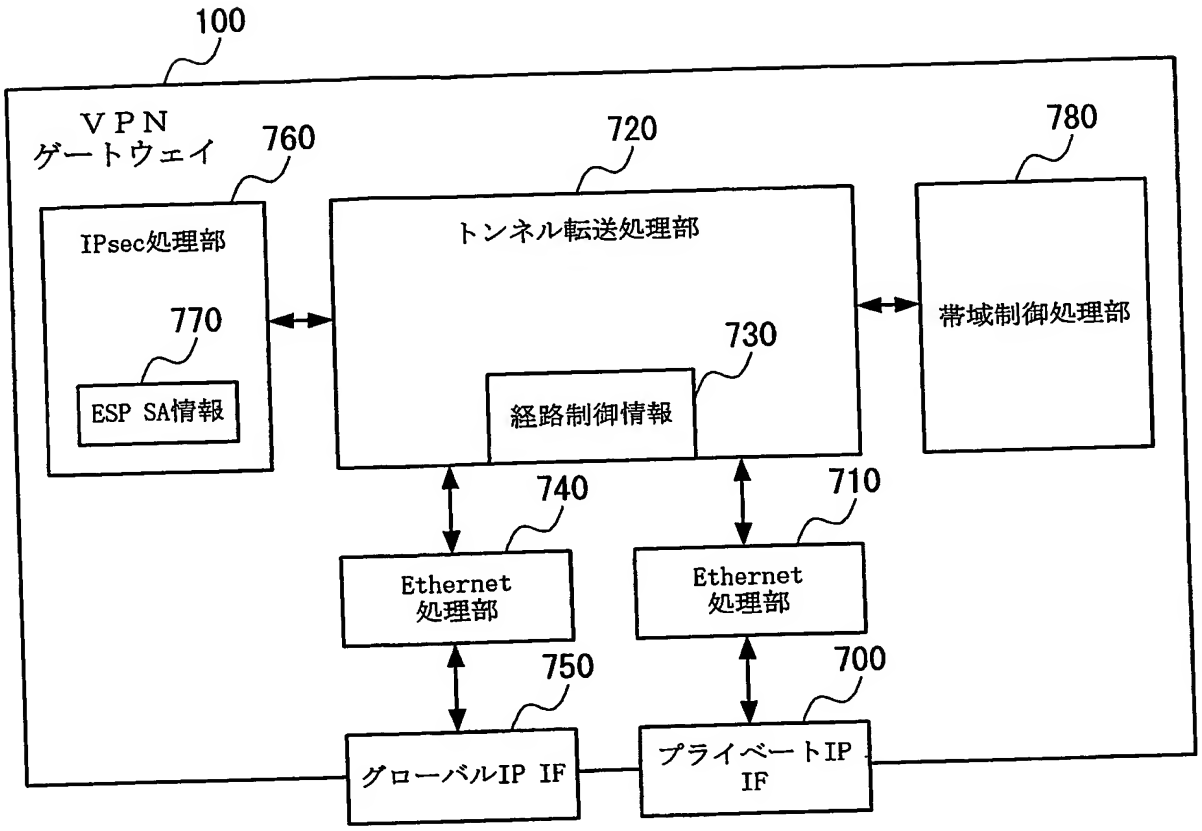
【図３】


70
無線基地制御局
360
移動無線通信制御部
330
移動無線通信プロトコル処理部
340
シグナリング処理部
350
ユーザデータ処理部
440
帯域制御処理部
320
430
IPトランスポート処理部
370
Ｌ４処理部
380
410
IPsec処理部
Ｌ２処理部
IP処理部
420
ESP SA情報
400
Ｌ２処理部
300
310
移動通信コア側IF
インターネット側IF

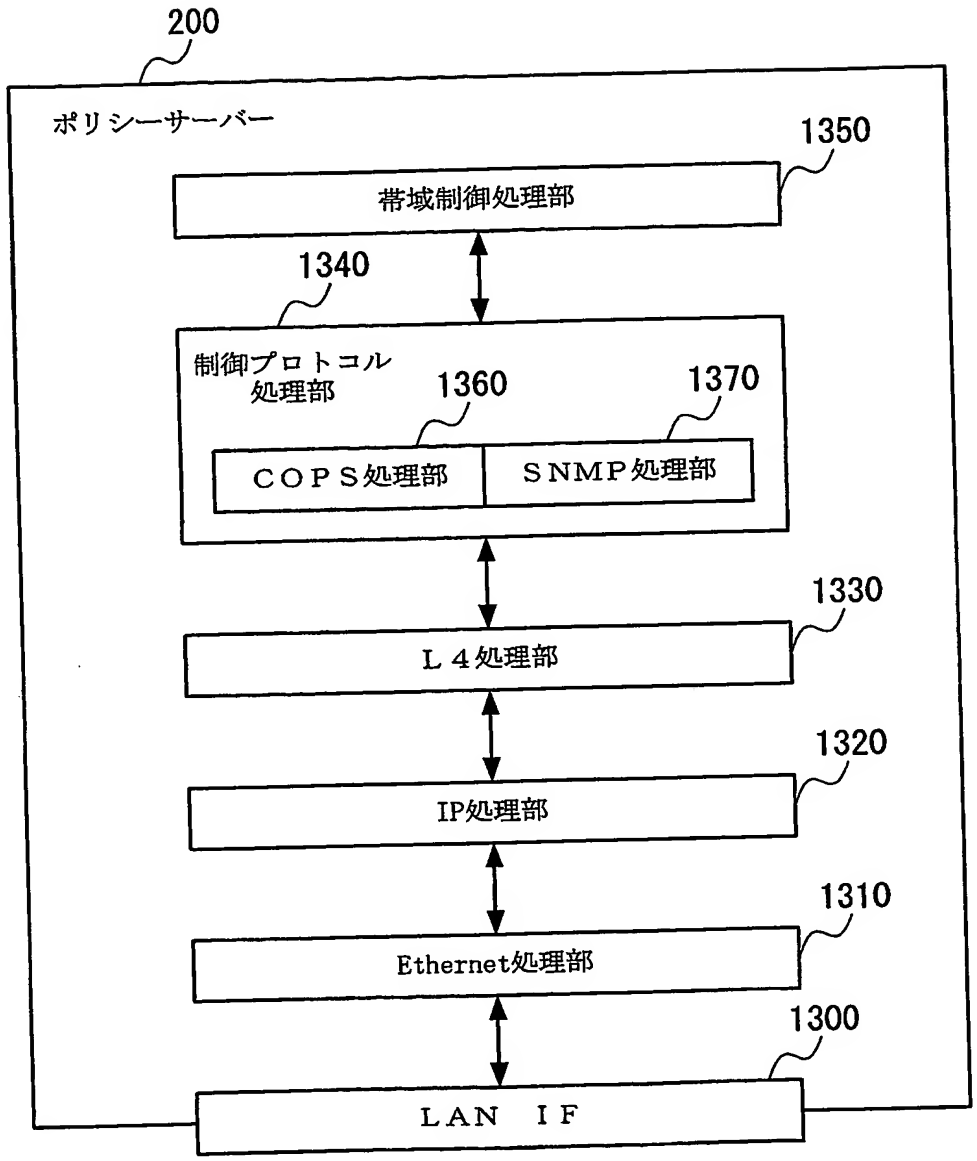
【図４】


60
無線基地局
移動無線通信制御部
530
移動無線通信プロトコル処理部
540
550
シグナリング処理部
ユーザデータ処理部
630
520
IPトランスポート処理部
570
Ｌ４処理部
610
580
IPsec処理部
620
ESP SA情報
IP処理部
Ｌ２処理部
600
Ethernet処理部
500
510
ＬＡＮ側
IF
無線側
IF

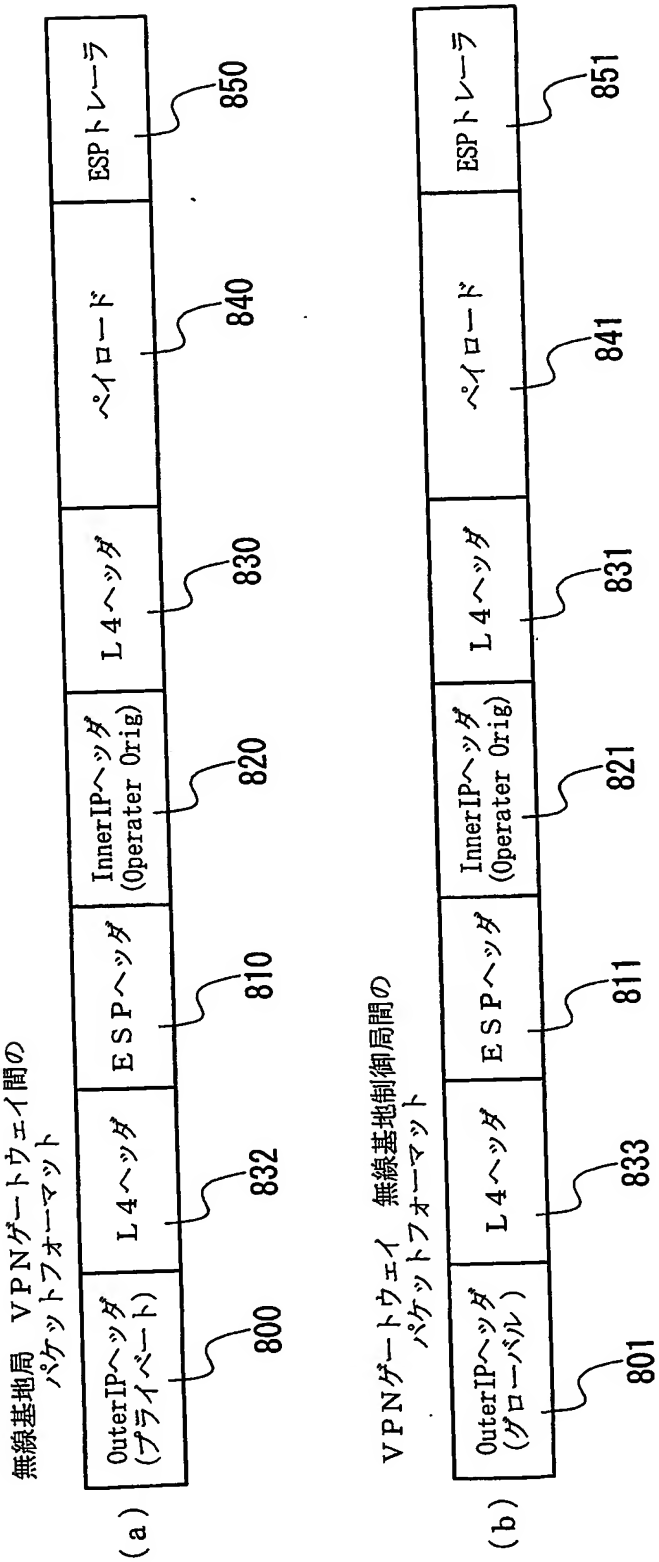
【図５】


100
ＶＰＮ
ゲートウェイ
760
IPsec処理部
770
ESP SA情報
720
トンネル転送処理部
730
経路制御情報
780
帯域制御処理部
740
Ethernet
処理部
710
Ethernet
処理部
750
700
グローバルIP IF
プライベートIP
IF

【図６】


200
ポリシーサーバー
1350
帯域制御処理部
1340
制御プロトコル
処理部
1360
1370
ＣＯＰＳ処理部
ＳＮＭＰ処理部
1330
Ｌ４処理部
1320
IP処理部
1310
Ethernet処理部
1300
ＬＡＮ　ＩＦ

【図７】

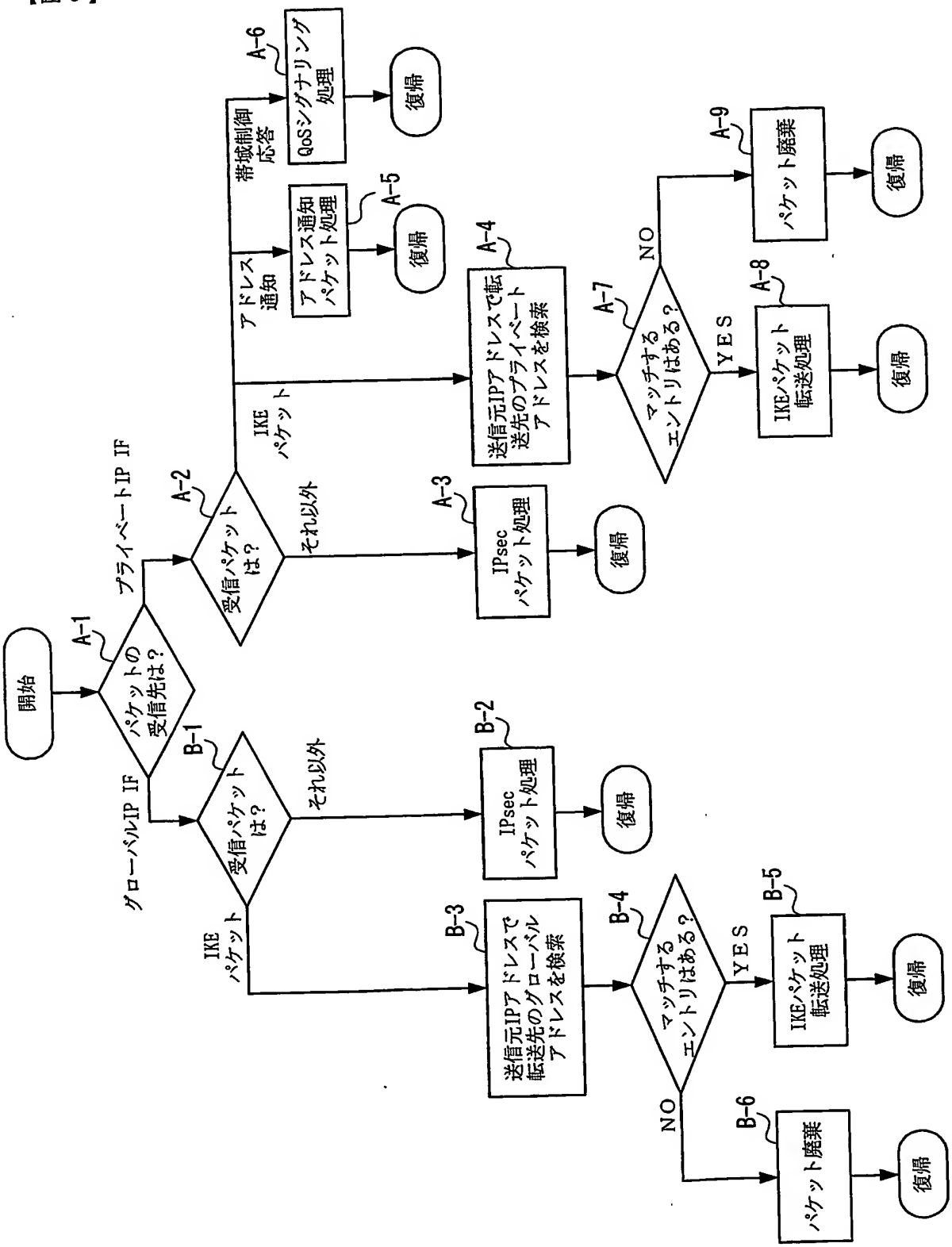

無線基地局　ＶＰＮゲートウェイ間の
パケットフォーマット
(a)
OuterIPヘッダ
(プライベート)
800
Ｌ４ヘッダ
832
ＥＳＰヘッダ
810
InnerIPヘッダ
(Operater Orig)
820
Ｌ４ヘッダ
830
ペイロード
840
ESPトレーラ
850
ＶＰＮゲートウェイ　無線基地制御局間の
パケットフォーマット
(b)
OuterIPヘッダ
(グローバル)
801
Ｌ４ヘッダ
833
ＥＳＰヘッダ
811
InnerIPヘッダ
(Operater Orig)
821
Ｌ４ヘッダ
831
ペイロード
841
ESPトレーラ
851

【図８】

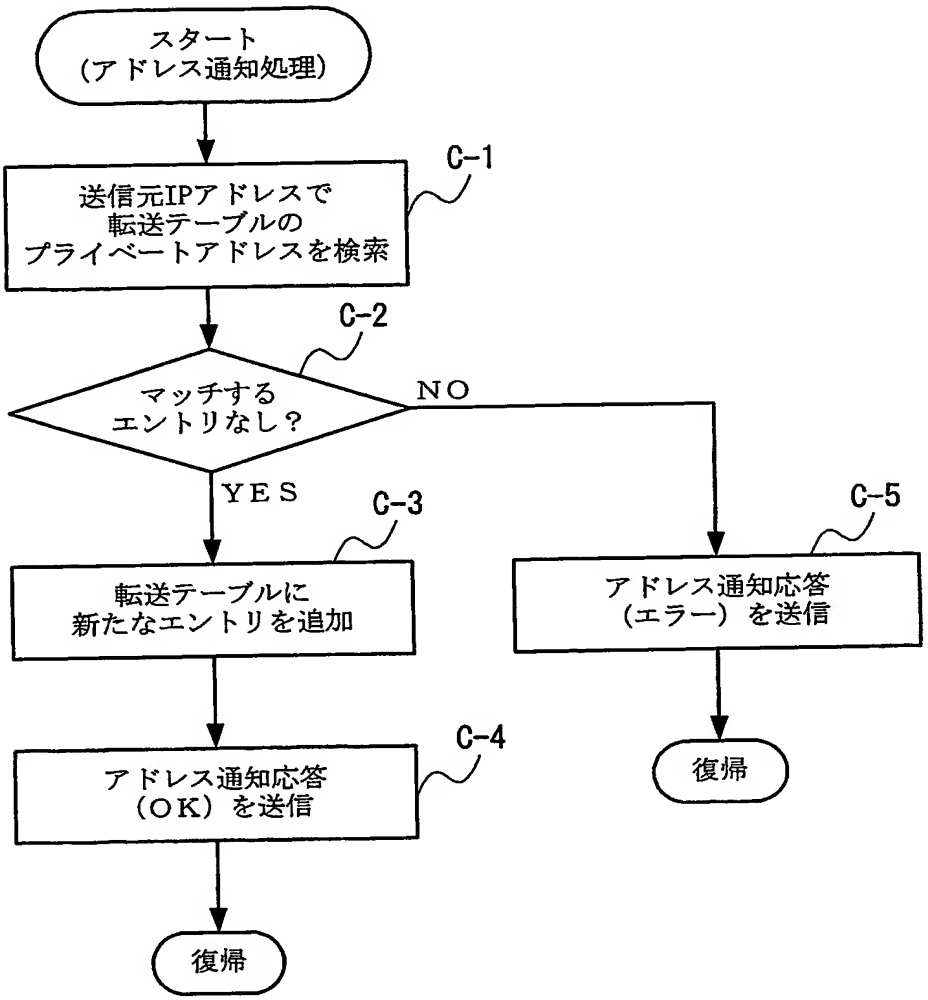
900 転送テーブル

無線基地制御局		無線基地局	
グローバル アドレス	オペレータ独自 アドレス	プライベート アドレス	オペレータ独自 アドレス
aaa. bbb. ccc. ddd	mmm. nnn. ooo. ppp	eee. fff. ggg. hhh	mmm. nnn. ooo. qqq
		eee. fff. ggg. kkk	mmm. nnn. ooo. rrr
		eee. fff. zzz. yyy	mmm. nnn. ooo. sss
		eee. fff. zzz. xxx	mmm. nnn. ooo. ttt

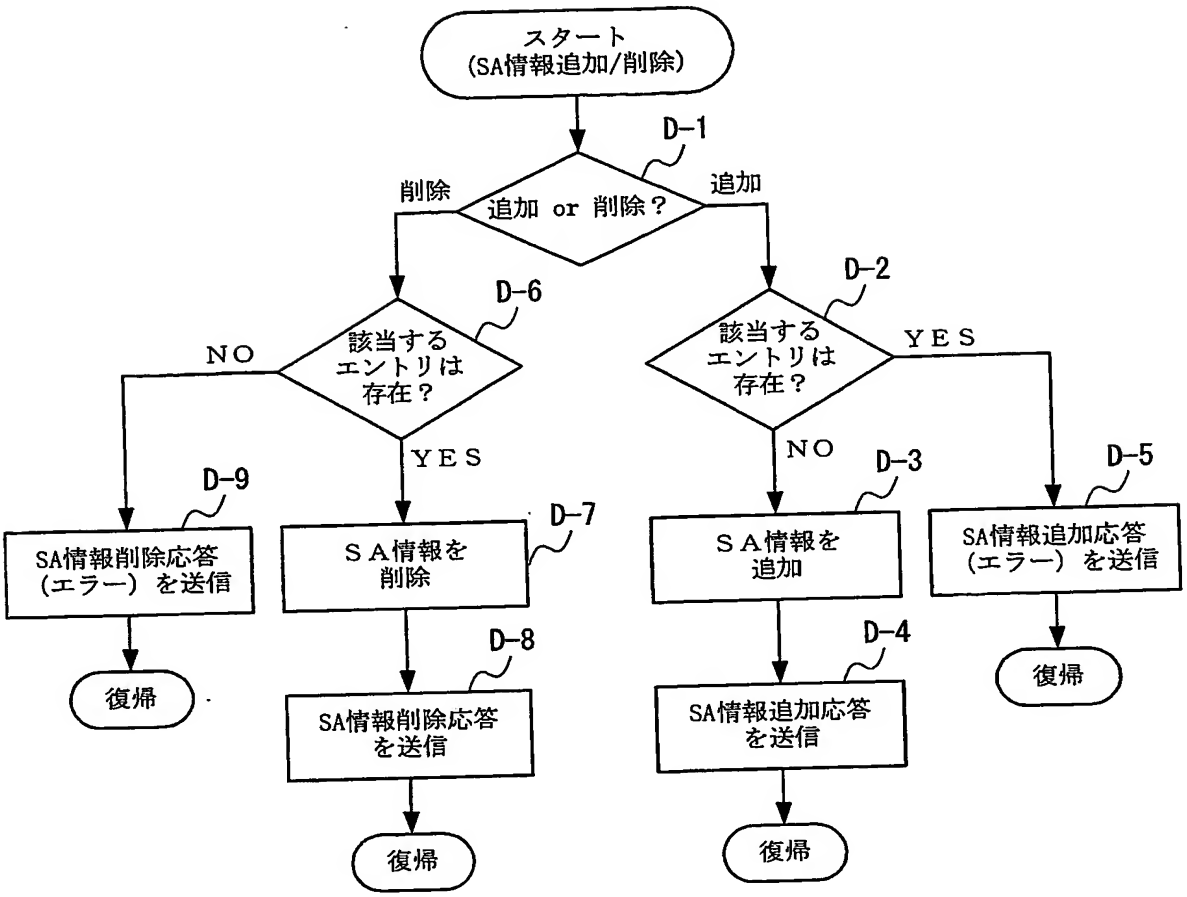
【図９】


開始
パケットの受信先は？
A-1
プライベートIP IF
グローバルIP IF
受信パケットは？
A-2
IKEパケット
それ以外
IPsecパケット処理
A-3
復帰
アドレス通知
帯域制御応答
アドレス通知パケット処理
A-5
復帰
QoSシグナリング処理
A-6
復帰
送信元IPアドレスで転送先のプライベートアドレスを検索
A-4
マッチするエントリはある？
A-7
NO
YES
パケット廃棄
A-9
復帰
IKEパケット転送処理
A-8
復帰
受信パケットは？
B-1
IKEパケット
それ以外
IPsecパケット処理
B-2
復帰
送信元IPアドレスで転送先のグローバルアドレスを検索
B-3
マッチするエントリはある？
B-4
NO
YES
パケット廃棄
B-6
復帰
IKEパケット転送処理
B-5
復帰

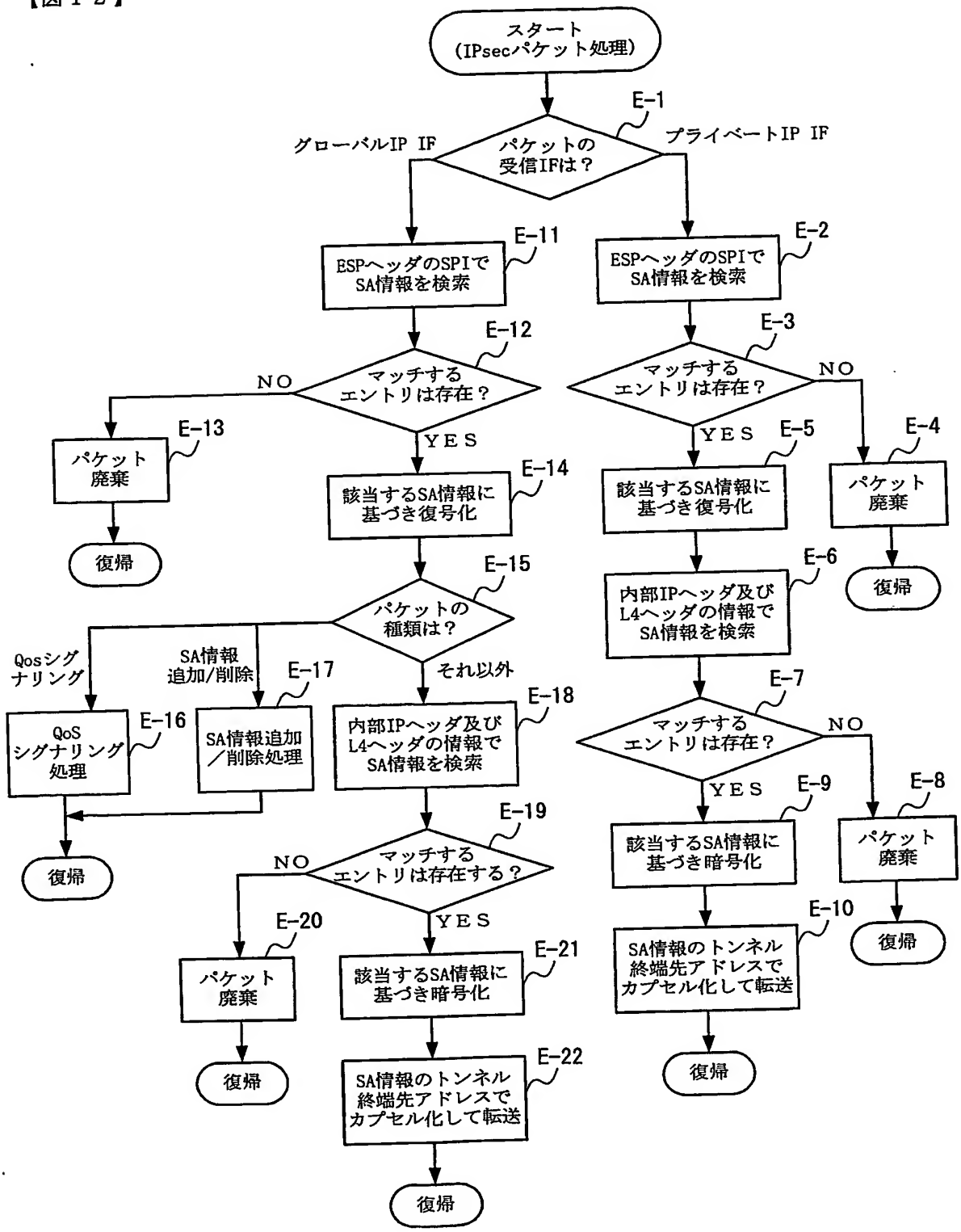
【図１０】


スタート
(アドレス通知処理)
C-1
送信元IPアドレスで
転送テーブルの
プライベートアドレスを検索
C-2
マッチする
エントリなし？
NO
YES
C-3
転送テーブルに
新たなエントリを追加
C-4
アドレス通知応答
（OK）を送信
復帰
C-5
アドレス通知応答
（エラー）を送信
復帰

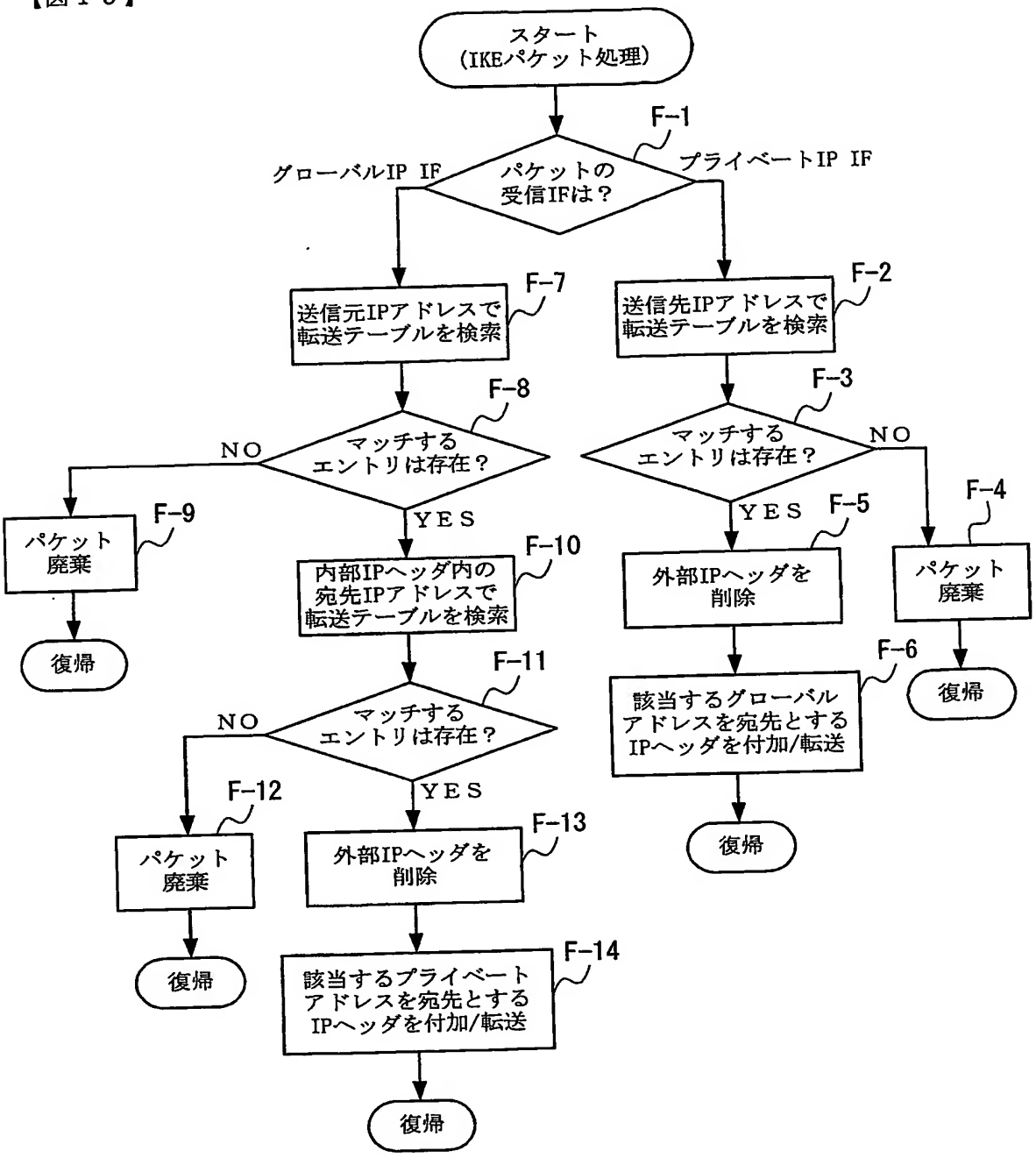
【図１１】


スタート
(SA情報追加/削除)
D-1
追加 or 削除？
削除
追加
D-6
該当する
エントリは
存在？
NO
YES
D-2
該当する
エントリは
存在？
YES
NO
D-9
SA情報削除応答
(エラー) を送信
D-7
ＳＡ情報を
削除
D-3
ＳＡ情報を
追加
D-5
SA情報追加応答
(エラー) を送信
復帰
D-8
SA情報削除応答
を送信
D-4
SA情報追加応答
を送信
復帰
復帰
復帰

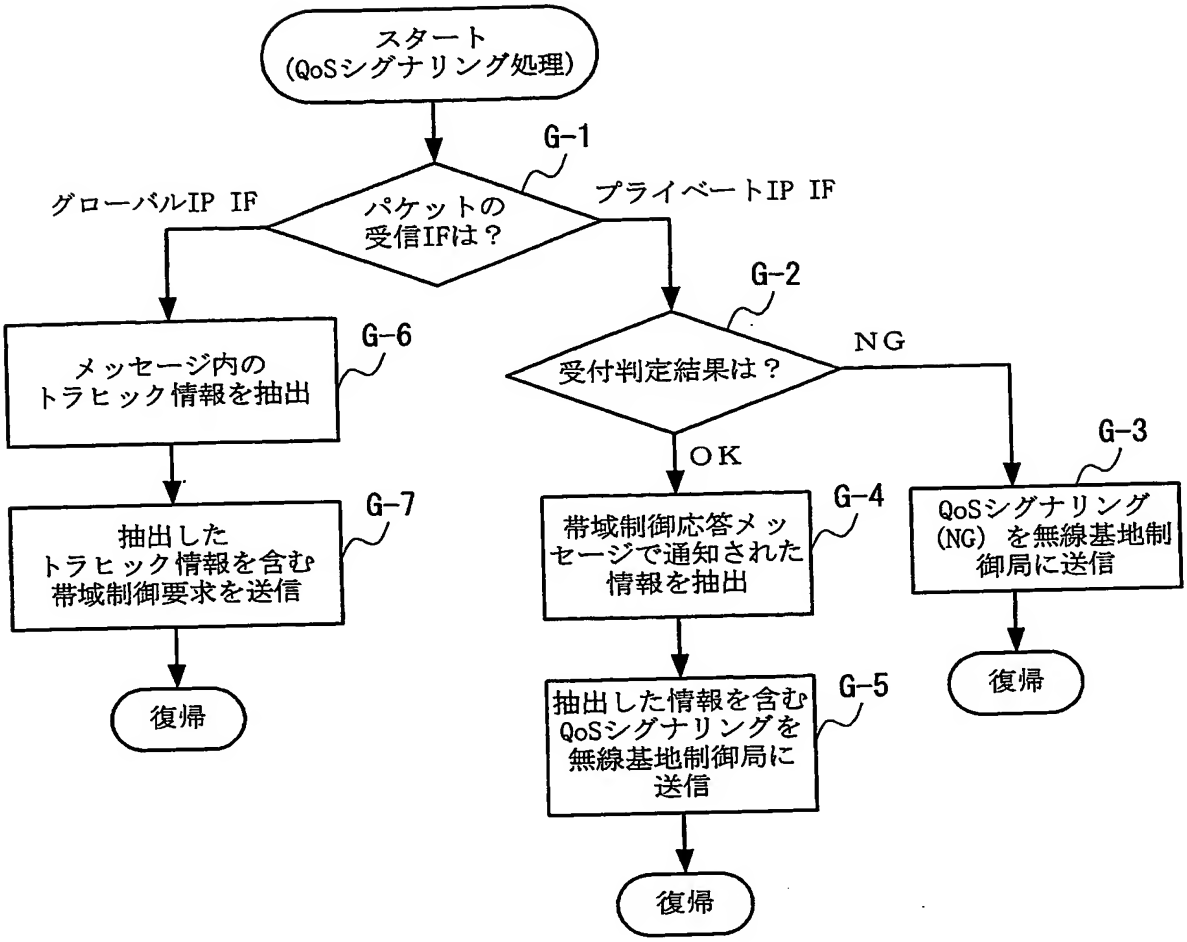
【図１２】


スタート
(IPsecパケット処理)
E-1
パケットの
受信IFは？
グローバルIP IF
プライベートIP IF
E-11
ESPヘッダのSPIで
SA情報を検索
E-2
ESPヘッダのSPIで
SA情報を検索
E-12
マッチする
エントリは存在？
NO
YES
E-3
マッチする
エントリは存在？
NO
YES
E-13
パケット
廃棄
復帰
E-14
該当するSA情報に
基づき復号化
E-5
該当するSA情報に
基づき復号化
E-4
パケット
廃棄
復帰
E-15
パケットの
種類は？
Qosシグ
ナリング
SA情報
追加/削除
それ以外
E-6
内部IPヘッダ及び
L4ヘッダの情報で
SA情報を検索
E-16
QoS
シグナリング
処理
E-17
SA情報追加
／削除処理
E-18
内部IPヘッダ及び
L4ヘッダの情報で
SA情報を検索
E-7
マッチする
エントリは存在？
NO
YES
E-9
該当するSA情報に
基づき暗号化
E-8
パケット
廃棄
復帰
復帰
E-19
マッチする
エントリは存在する？
NO
YES
E-10
SA情報のトンネル
終端先アドレスで
カプセル化して転送
復帰
E-20
パケット
廃棄
復帰
E-21
該当するSA情報に
基づき暗号化
E-22
SA情報のトンネル
終端先アドレスで
カプセル化して転送
復帰

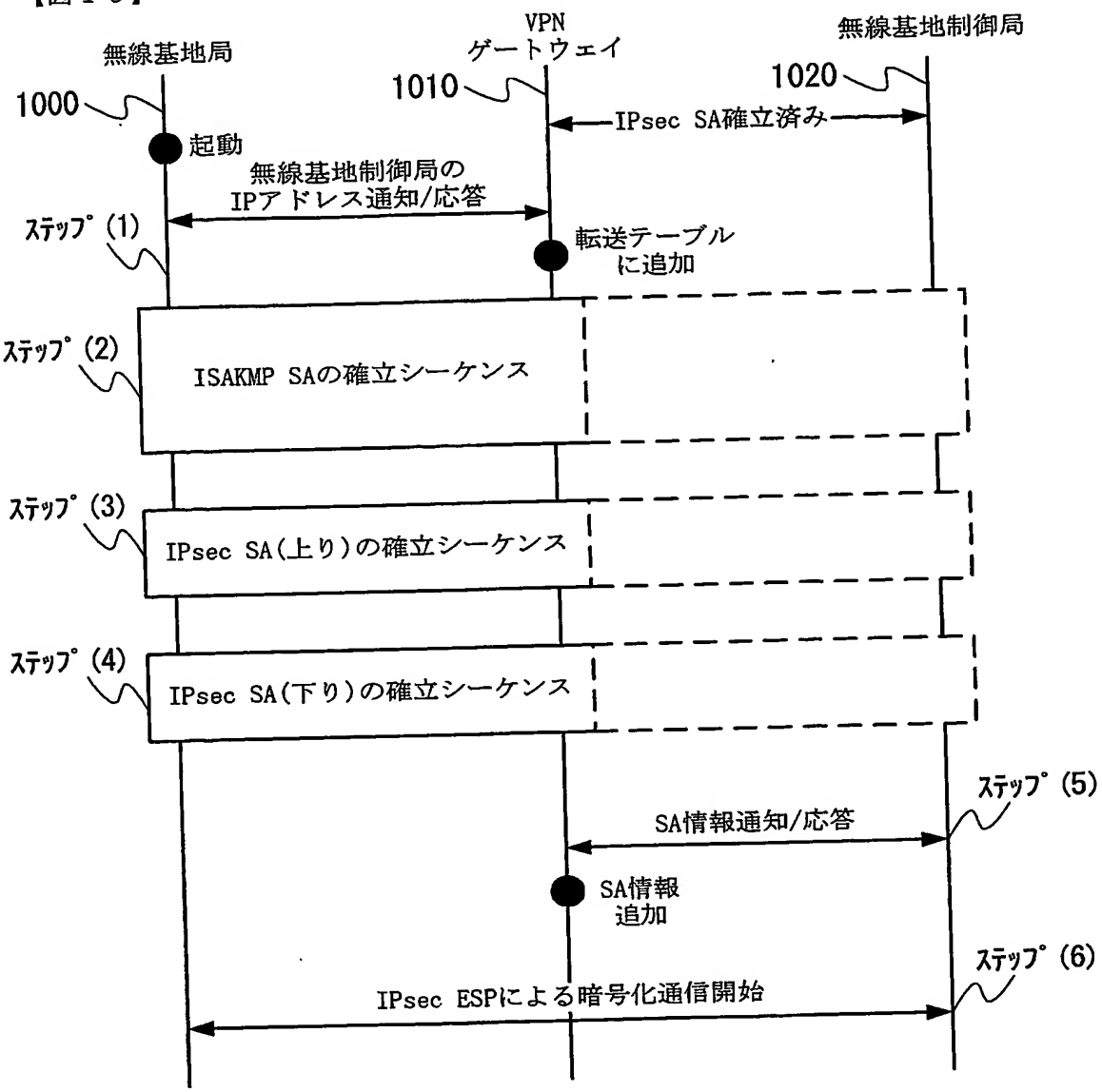
【図１３】


スタート
(IKEパケット処理)
F-1
パケットの
受信IFは？
グローバルIP IF
プライベートIP IF
F-7
送信元IPアドレスで
転送テーブルを検索
F-2
送信先IPアドレスで
転送テーブルを検索
F-8
マッチする
エントリは存在？
NO
YES
F-3
マッチする
エントリは存在？
NO
YES
F-9
パケット
廃棄
復帰
F-10
内部IPヘッダ内の
宛先IPアドレスで
転送テーブルを検索
F-5
外部IPヘッダを
削除
F-4
パケット
廃棄
復帰
F-11
マッチする
エントリは存在？
NO
YES
F-6
該当するグローバル
アドレスを宛先とする
IPヘッダを付加/転送
復帰
F-12
パケット
廃棄
復帰
F-13
外部IPヘッダを
削除
F-14
該当するプライベート
アドレスを宛先とする
IPヘッダを付加/転送
復帰

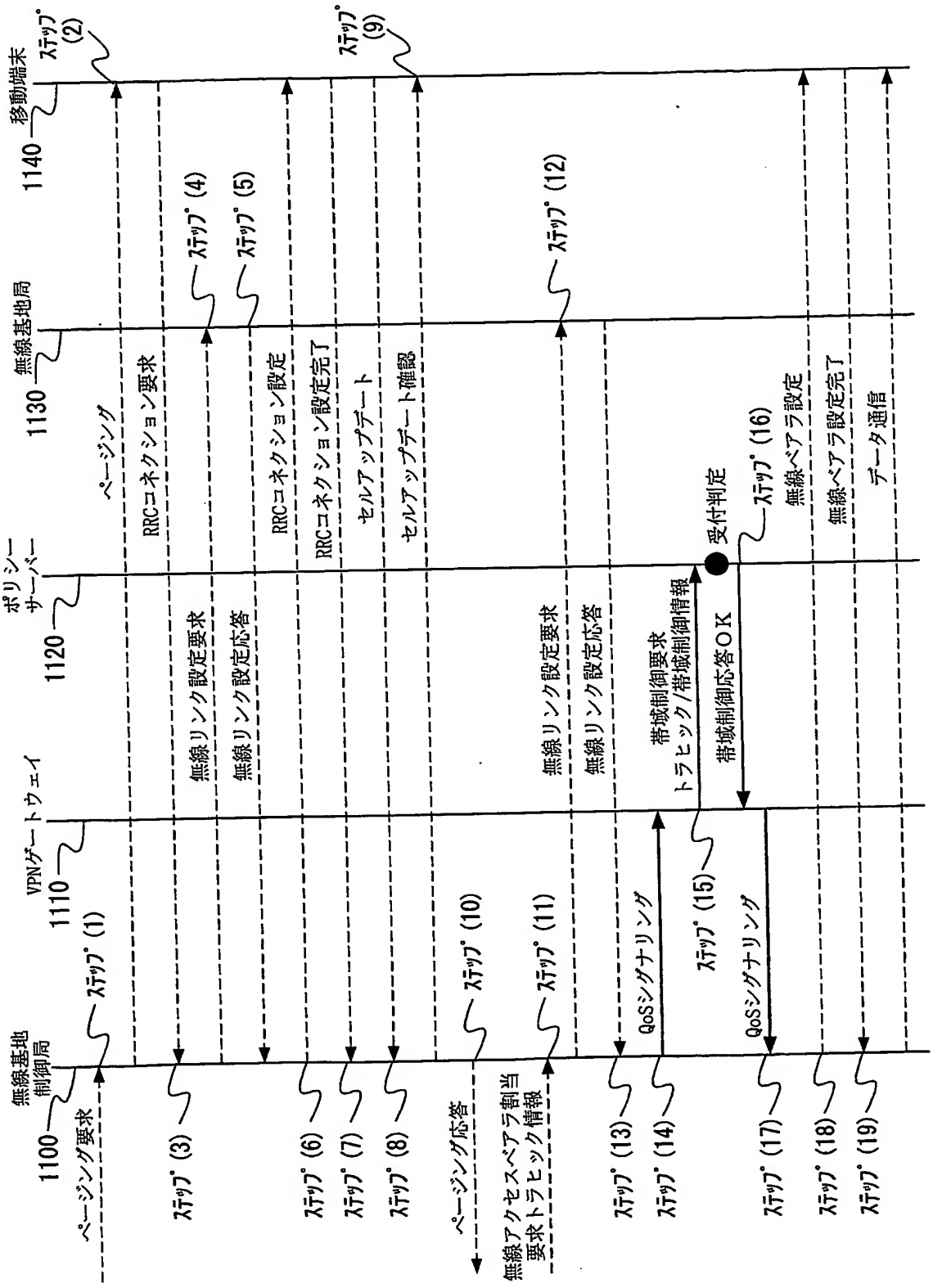
【図１４】


スタート
(QoSシグナリング処理)
G-1
パケットの
受信IFは？
グローバルIP IF
プライベートIP IF
G-2
受付判定結果は？
NG
OK
G-6
メッセージ内の
トラヒック情報を抽出
G-7
抽出した
トラヒック情報を含む
帯域制御要求を送信
復帰
G-4
帯域制御応答メッ
セージで通知された
情報を抽出
G-5
抽出した情報を含む
QoSシグナリングを
無線基地制御局に
送信
復帰
G-3
QoSシグナリング
(NG) を無線基地制
御局に送信
復帰

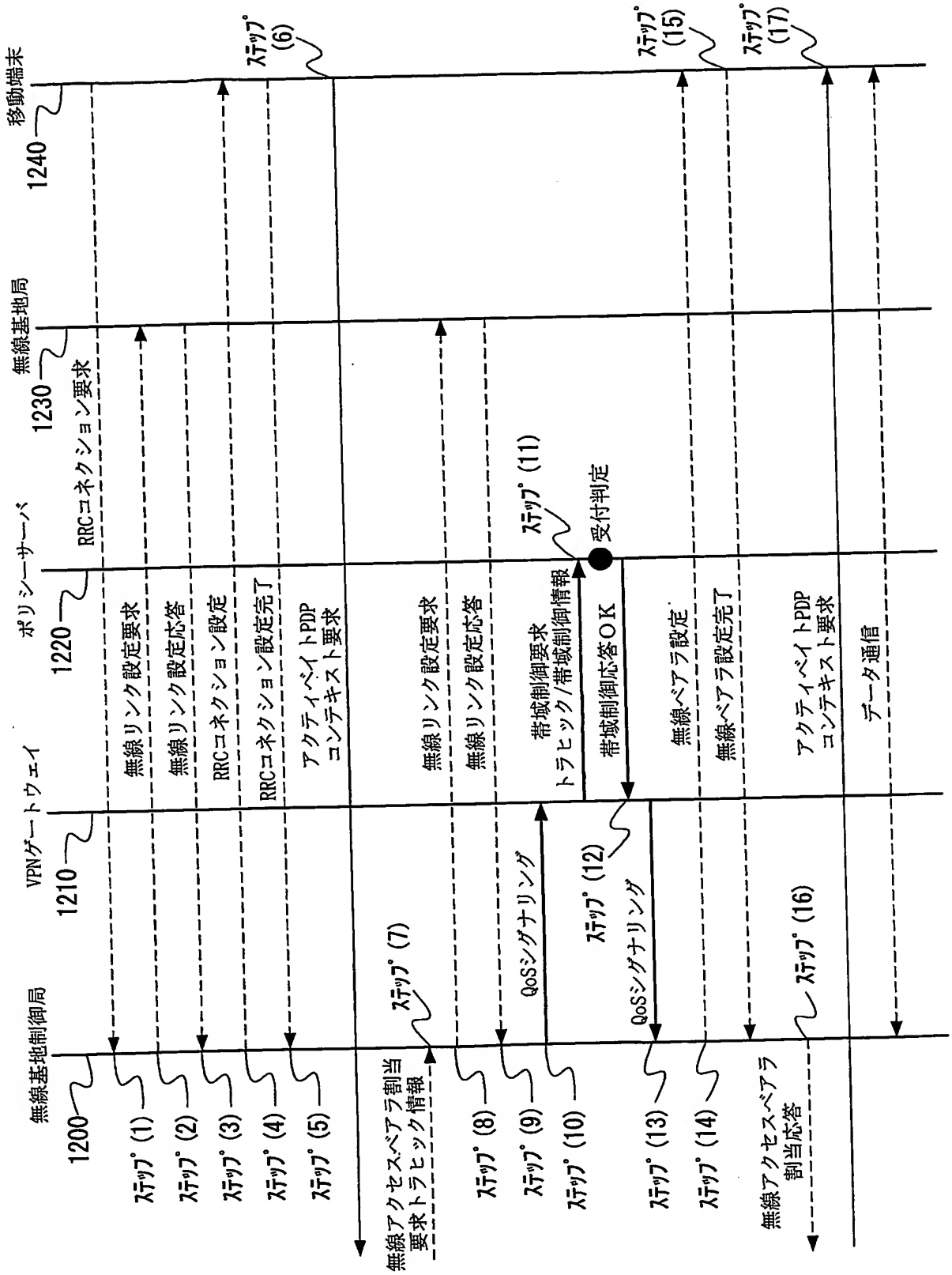
【図１５】


無線基地局
VPN
ゲートウェイ
無線基地制御局
1000
1010
1020
IPsec SA確立済み
起動
無線基地制御局の
IPアドレス通知/応答
ステップ(1)
転送テーブル
に追加
ステップ(2)
ISAKMP SAの確立シーケンス
ステップ(3)
IPsec SA(上り)の確立シーケンス
ステップ(4)
IPsec SA(下り)の確立シーケンス
ステップ(5)
SA情報通知/応答
SA情報
追加
ステップ(6)
IPsec ESPによる暗号化通信開始

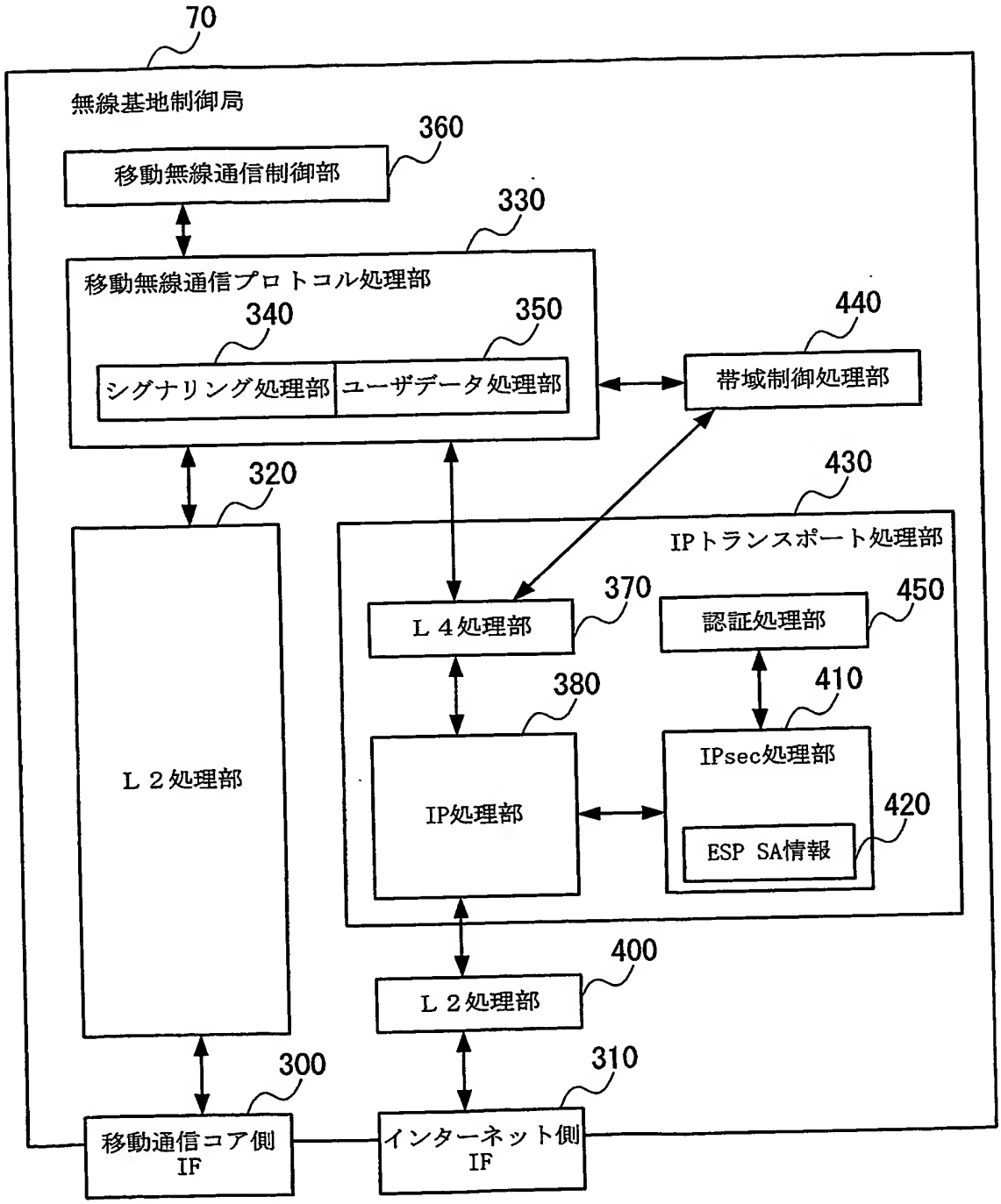
【図１６】


無線基地制御局
1100
VPNゲートウェイ
1110
ポリシーサーバー
1120
無線基地局
1130
移動端末
1140
ページング要求
ステップ(1)
ページング
ステップ(2)
ステップ(3)
RRCコネクション要求
無線リンク設定要求
ステップ(4)
無線リンク設定応答
ステップ(5)
RRCコネクション設定
ステップ(6)
RRCコネクション設定完了
ステップ(7)
セルアップデート
ステップ(8)
セルアップデート確認
ステップ(9)
ページング応答
ステップ(10)
無線アクセスベアラ割当要求トラヒック情報
ステップ(11)
無線リンク設定要求
無線リンク設定応答
ステップ(12)
ステップ(13)
QoSシグナリング
ステップ(14)
帯域制御要求
トラヒック/帯域制御情報
ステップ(15)
受付判定
帯域制御応答OK
ステップ(16)
QoSシグナリング
ステップ(17)
無線ベアラ設定
ステップ(18)
無線ベアラ設定完了
ステップ(19)
データ通信

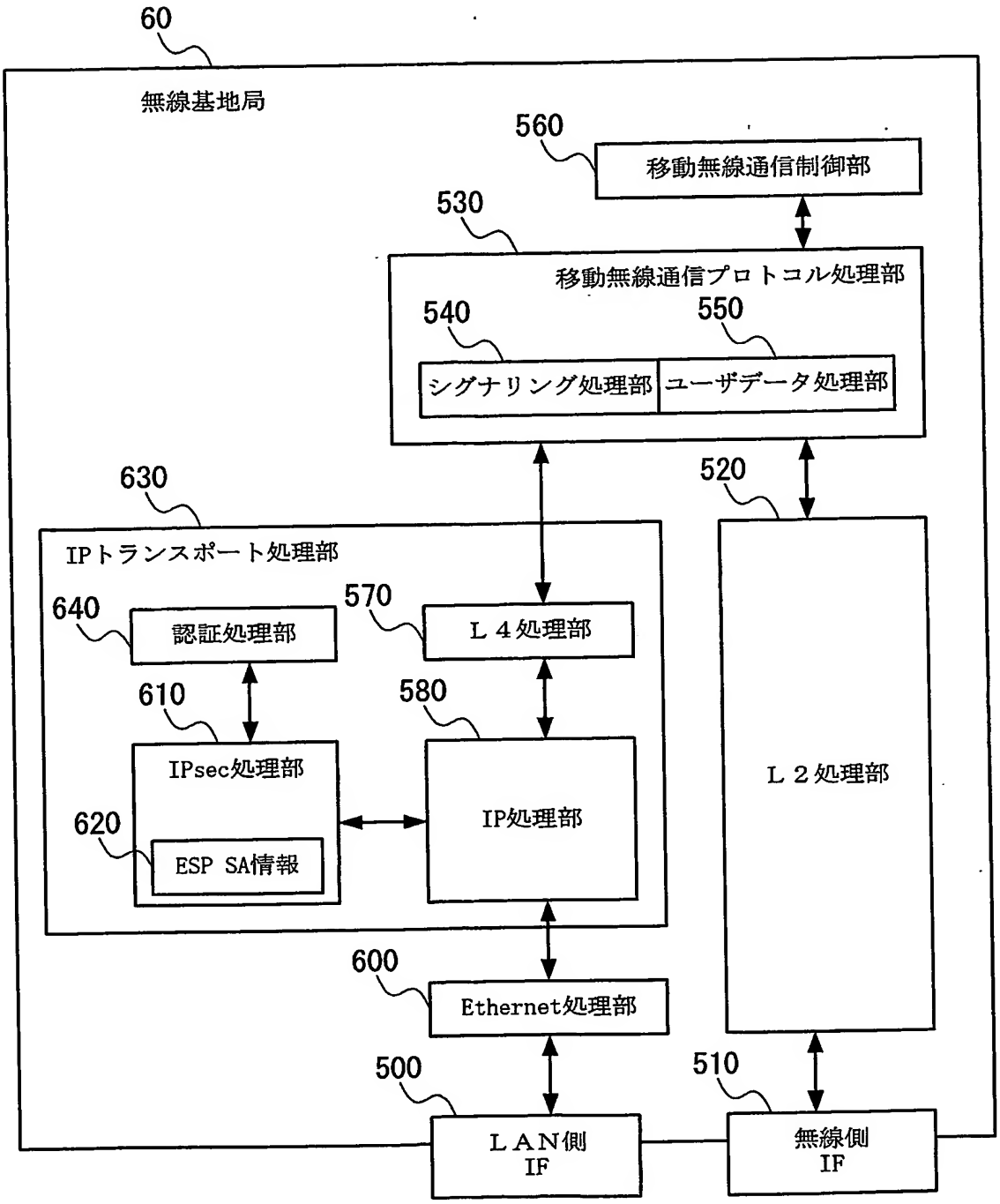
【図１７】


無線基地制御局
1200
VPNゲートウェイ
1210
ポリシーサーバ
1220
無線基地局
1230
移動端末
1240
ステップ (1)
無線リンク設定要求
ステップ (2)
無線リンク設定応答
ステップ (3)
RRCコネクション設定
ステップ (4)
RRCコネクション設定完了
ステップ (5)
アクティベイトPDP
コンテキスト要求
ステップ (6)
ステップ (7)
無線アクセスベアラ割当
要求トラヒック情報
ステップ (8)
無線リンク設定要求
ステップ (9)
無線リンク設定応答
ステップ (10)
QoSシグナリング
ステップ (11)
帯域制御要求
トラヒック/帯域制御情報
受付判定
ステップ (12)
帯域制御応答OK
QoSシグナリング
ステップ (13)
無線ベアラ設定
ステップ (14)
無線ベアラ設定完了
ステップ (15)
ステップ (16)
無線アクセスベアラ
割当応答
アクティベイトPDP
コンテキスト要求
ステップ (17)
データ通信

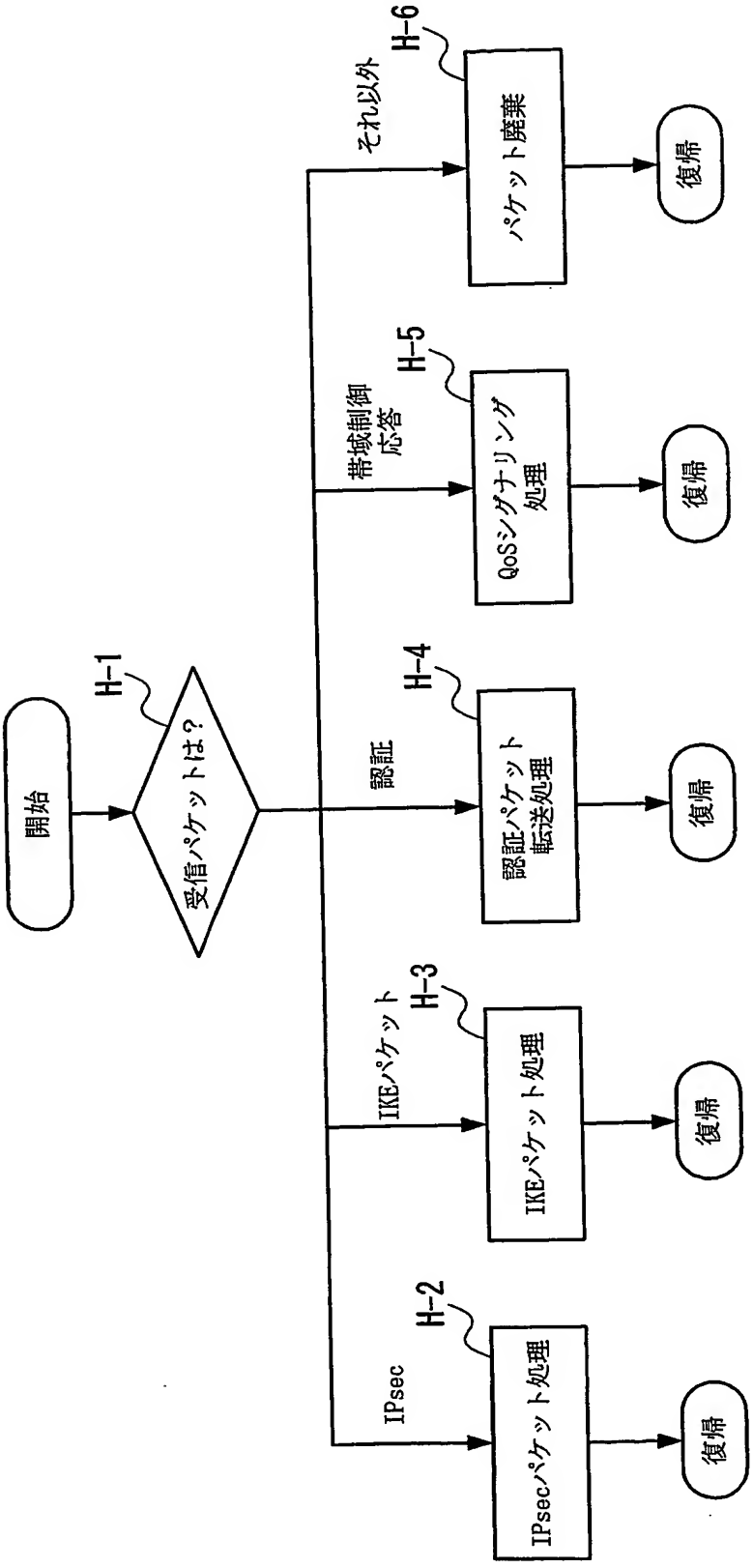
【図１８】


70
無線基地制御局
360
移動無線通信制御部
330
移動無線通信プロトコル処理部
340
シグナリング処理部
350
ユーザデータ処理部
440
帯域制御処理部
320
430
IPトランスポート処理部
370
Ｌ４処理部
450
認証処理部
380
410
IPsec処理部
Ｌ２処理部
IP処理部
420
ESP SA情報
400
Ｌ２処理部
300
310
移動通信コア側IF
インターネット側IF

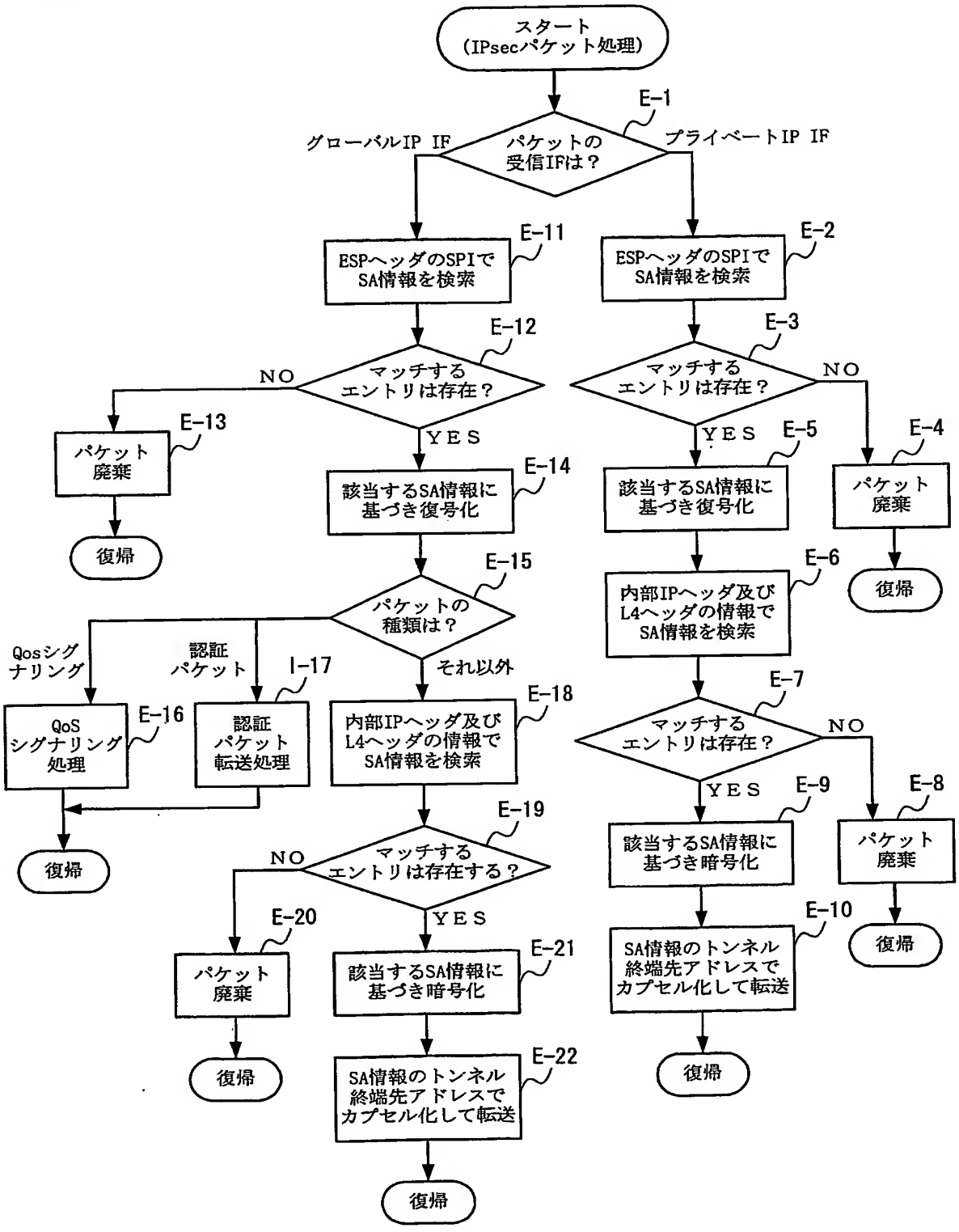
【図１９】


60
無線基地局
560
移動無線通信制御部
530
移動無線通信プロトコル処理部
540
550
シグナリング処理部
ユーザデータ処理部
630
520
IPトランスポート処理部
640
認証処理部
570
Ｌ４処理部
610
580
IPsec処理部
620
ESP SA情報
IP処理部
Ｌ２処理部
600
Ethernet処理部
500
510
ＬＡＮ側
IF
無線側
IF

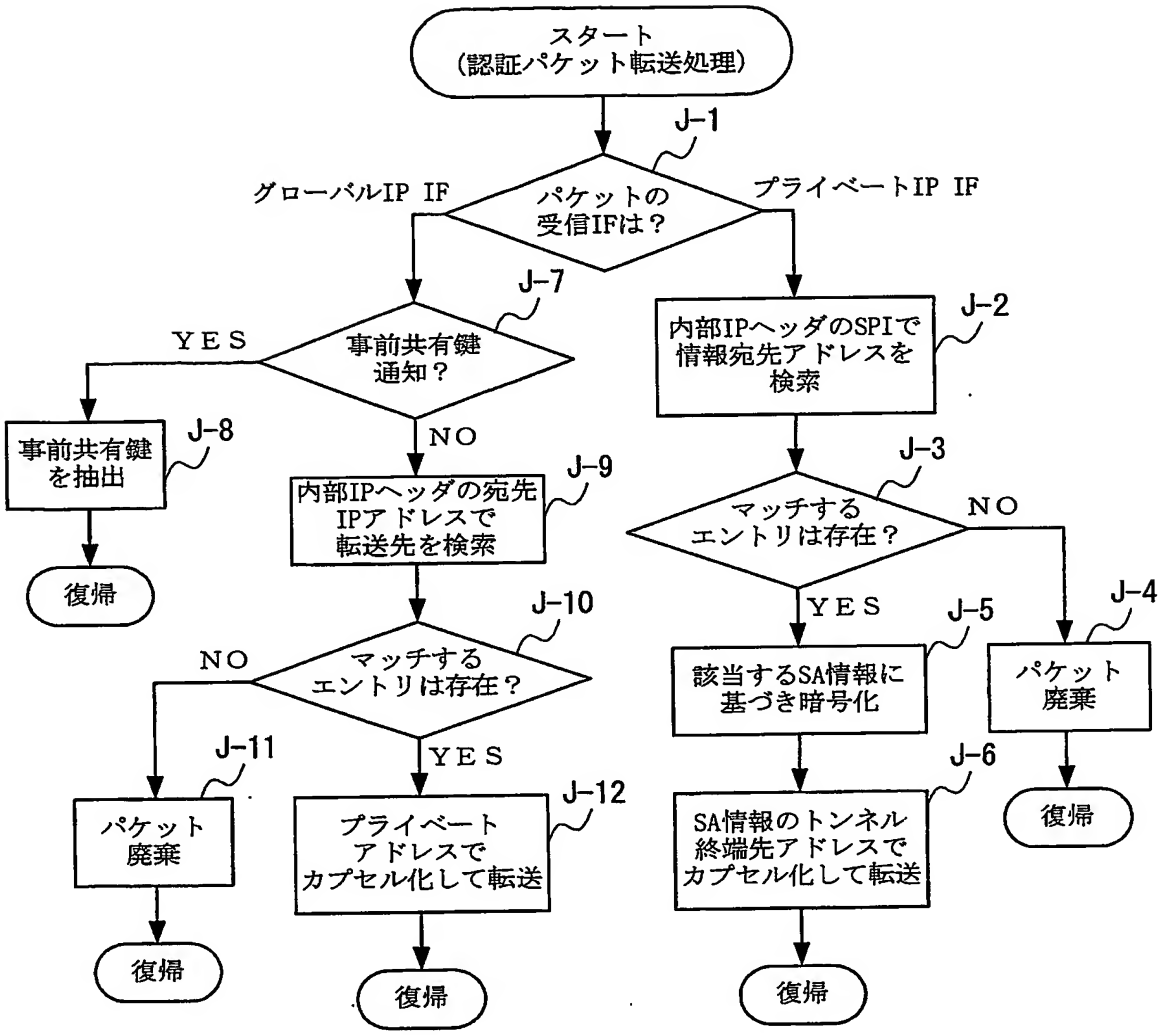
【図２０】


開始
H-1
受信パケットは？
認証
H-4
認証パケット転送処理
復帰
帯域制御応答
H-5
QoSシグナリング処理
復帰
それ以外
H-6
パケット廃棄
復帰
IKEパケット
H-3
IKEパケット処理
復帰
IPsec
H-2
IPsecパケット処理
復帰

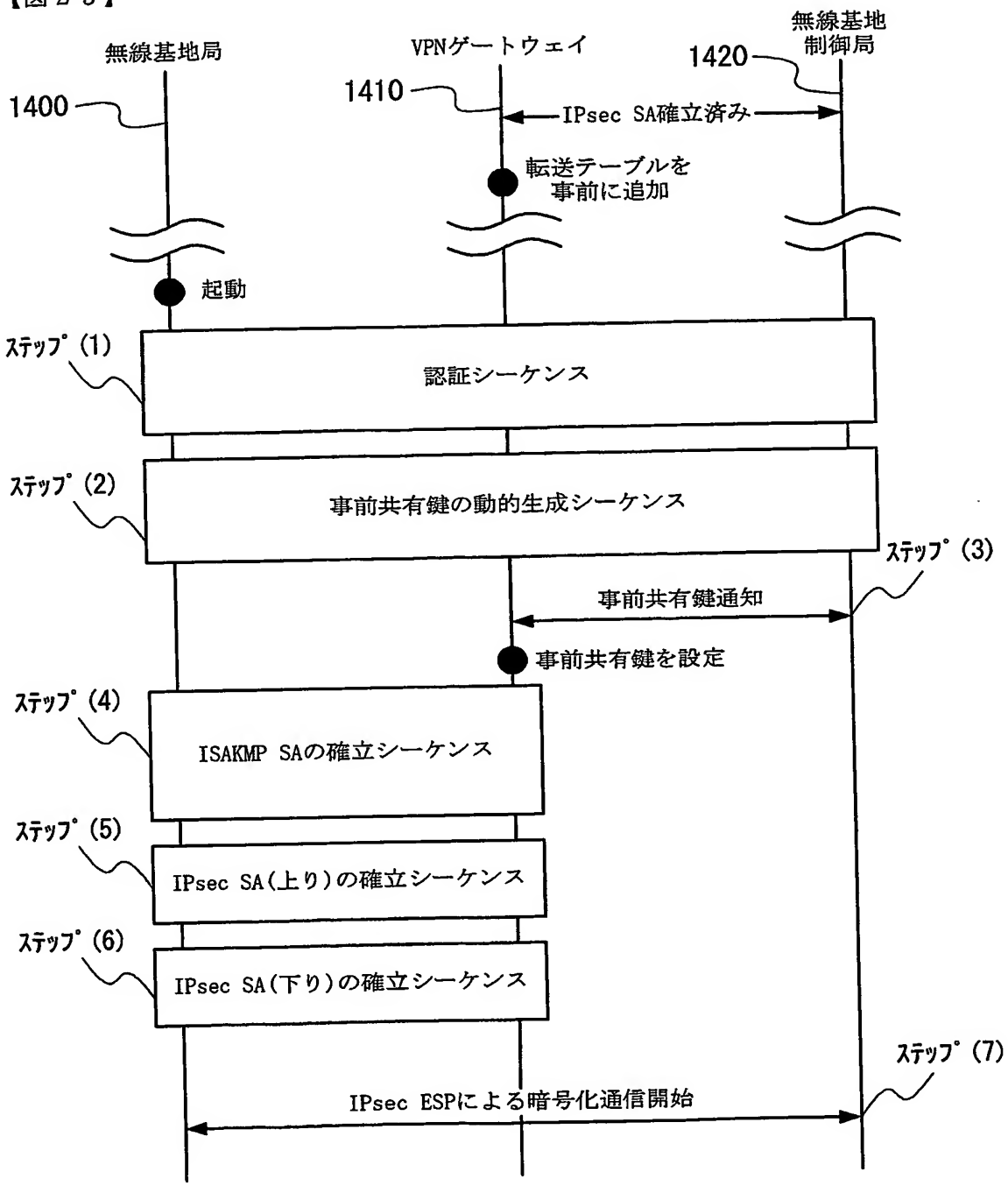
【図２１】


スタート
(IPsecパケット処理)
E-1
パケットの
受信IFは？
グローバルIP IF
プライベートIP IF
ESPヘッダのSPIで
SA情報を検索
E-11
ESPヘッダのSPIで
SA情報を検索
E-2
E-12
マッチする
エントリは存在？
NO
YES
E-3
マッチする
エントリは存在？
NO
YES
パケット
廃棄
E-13
該当するSA情報に
基づき復号化
E-14
該当するSA情報に
基づき復号化
E-5
パケット
廃棄
E-4
復帰
復帰
E-15
パケットの
種類は？
Qosシグ
ナリング
認証
パケット
それ以外
I-17
内部IPヘッダ及び
L4ヘッダの情報で
SA情報を検索
E-6
QoS
シグナリング
処理
E-16
認証
パケット
転送処理
内部IPヘッダ及び
L4ヘッダの情報で
SA情報を検索
E-18
E-7
マッチする
エントリは存在？
NO
YES
E-9
E-8
該当するSA情報に
基づき暗号化
パケット
廃棄
復帰
E-19
マッチする
エントリは存在する？
NO
YES
E-10
SA情報のトンネル
終端先アドレスで
カプセル化して転送
復帰
E-20
パケット
廃棄
該当するSA情報に
基づき暗号化
E-21
復帰
SA情報のトンネル
終端先アドレスで
カプセル化して転送
E-22
復帰

【図２２】


スタート
(認証パケット転送処理)
J-1
パケットの
受信IFは？
グローバルIP IF
プライベートIP IF
J-7
事前共有鍵
通知？
YES
NO
J-8
事前共有鍵
を抽出
復帰
J-9
内部IPヘッダの宛先
IPアドレスで
転送先を検索
J-10
マッチする
エントリは存在？
NO
YES
J-11
パケット
廃棄
復帰
J-12
プライベート
アドレスで
カプセル化して転送
復帰
J-2
内部IPヘッダのSPIで
情報宛先アドレスを
検索
J-3
マッチする
エントリは存在？
NO
YES
J-4
パケット
廃棄
復帰
J-5
該当するSA情報に
基づき暗号化
J-6
SA情報のトンネル
終端先アドレスで
カプセル化して転送
復帰

【図２３】


無線基地局
VPNゲートウェイ
無線基地制御局
1400
1410
1420
IPsec SA確立済み
転送テーブルを事前に追加
起動
ステップ(1)
認証シーケンス
ステップ(2)
事前共有鍵の動的生成シーケンス
ステップ(3)
事前共有鍵通知
事前共有鍵を設定
ステップ(4)
ISAKMP SAの確立シーケンス
ステップ(5)
IPsec SA(上り)の確立シーケンス
ステップ(6)
IPsec SA(下り)の確立シーケンス
ステップ(7)
IPsec ESPによる暗号化通信開始

【書類名】要約書
【要約】
【課題】　私設網を用いて移動通信サービスを提供するに当たり、移動通信トラヒックの増大に起因して私設網内回線が輻輳するのを防ぎ、他のトラヒックにも支障をきたさない移動通信システムを提供する。
【解決手段】　移動端末８０の発呼あるいは着呼時に、移動通信制御シグナリングを受信した中継ノードであるＶＰＮゲートウェイ１００が私設網であるＬＡＮ２０内の帯域制御機構と連携して受け付け判定を行い、受付が許可された場合のみ、移動端末８０に通信回線を提供し、あるいは、無線基地局６０と無線基地制御局７０間で鍵交換メカニズムにより動的に事前共有鍵を生成し、無線基地制御局７０がＶＰＮゲートウェイ１００に事前共有鍵を通知する。
【選択図】　図２

認定・付加情報

特許出願の番号	特願２００３－３９０２１６
受付番号	５０３０１９１４３８４
書類名	特許願
担当官	第七担当上席　００９６
作成日	平成１５年１１月２１日

＜認定情報・付加情報＞

【提出日】　平成15年11月20日

特願２００３－３９０２１６

出　願　人　履　歴　情　報

識別番号　［０００００４２３７］

１．変更年月日　１９９０年　８月２９日
［変更理由］　新規登録
住　所　東京都港区芝五丁目７番１号
氏　名　日本電気株式会社